

# The finite harmonic oscillator and its applications to sequences, communication and radar

Shamgar Gurevich, Ronny Hadani and Nir Sochen

**Abstract**—A novel system, called the *oscillator system*, consisting of order of  $p^3$  functions (signals) on the finite field  $\mathbb{F}_p$ , with  $p$  an odd prime, is described and studied. The new functions are proved to satisfy good auto-correlation, cross-correlation and low peak-to-average power ratio properties. Moreover, the oscillator system is closed under the operation of discrete Fourier transform. Applications of the oscillator system for discrete radar and digital communication theory are explained. Finally, an explicit algorithm to construct the oscillator system is presented.

**Index Terms**—Weil representation, commutative subgroups, eigenfunctions, good correlations, low supremum, Fourier invariance, explicit algorithm.

## I. INTRODUCTION

ONE-dimensional *analog signals* are complex valued functions on the real line  $\mathbb{R}$ . In the same spirit, one-dimensional *digital signals*, also called *sequences*, might be considered as complex valued functions on the finite line  $\mathbb{F}_p$ , i.e., the finite field with  $p$  elements. In both situations the parameter of the line is denoted by  $t$  and is referred to as *time*. In this work, we will consider digital signals only, which will be simply referred to as signals. The space of signals  $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$  is a Hilbert space with the Hermitian product given by

$$\langle \phi, \varphi \rangle = \sum_{t \in \mathbb{F}_p} \phi(t) \overline{\varphi(t)}.$$

A central problem is to construct interesting and useful systems of signals. Given a system  $\mathfrak{S}$ , there are various desired properties which appear in the engineering wish list. For example, in various situations [GG], [HCM] one requires that the signals will be weakly correlated, i.e., that for every  $\phi \neq \varphi \in \mathfrak{S}$

$$|\langle \phi, \varphi \rangle| \ll 1.$$

This property is trivially satisfied if  $\mathfrak{S}$  is an orthonormal basis. Such a system cannot consist of more than  $\dim(\mathcal{H})$  signals, however, for certain applications, e.g., CDMA (Code Division Multiple Access) [V] a larger number of signals is desired, in that case the orthogonality condition is relaxed.

During the transmission process, a signal  $\varphi$  might be distorted in various ways. Two basic types of distortions are *time shift*  $\varphi(t) \mapsto L_\tau \varphi(t) = \varphi(t + \tau)$  and *phase shift*

$\varphi(t) \mapsto M_w \varphi(t) = e^{\frac{2\pi i}{p} w t} \varphi(t)$ , where  $\tau, w \in \mathbb{F}_p$ . The first type appears in asynchronous communication and the second type is a Doppler effect due to relative velocity between the transmitting and receiving antennas. In conclusion, a general distortion is of the type  $\varphi \mapsto M_w L_\tau \varphi$ , suggesting that for every  $\varphi \neq \phi \in \mathfrak{S}$  it is natural to require [HCM] the following stronger condition

$$|\langle \phi, M_w L_\tau \varphi \rangle| \ll 1.$$

Due to technical restrictions in the transmission process, signals are sometimes required to admit low peak-to-average power ratio [PT], i.e., that for every  $\varphi \in \mathfrak{S}$  with  $\|\varphi\|_2 = 1$

$$\max \{|\varphi(t)| : t \in \mathbb{F}_p\} \ll 1.$$

Finally, several schemes for digital communication require that the above properties will continue to hold also if we replace signals from  $\mathfrak{S}$  by their Fourier transform.

In this paper we construct a novel system of (unit) signals  $\mathfrak{S}_O$ , consisting of order of  $p^3$  signals, where  $p$  is an odd prime, called the *oscillator system*. These signals constitute, in an appropriate formal sense, a finite analogue for the eigenfunctions of the harmonic oscillator in the real setting and, in accordance, they share many of the nice properties of the latter class. In particular, we will prove that  $\mathfrak{S}_O$  satisfies the following properties

- 1) *Autocorrelation (ambiguity function)*. For every  $\varphi \in \mathfrak{S}_O$  we have

$$|\langle \varphi, M_w L_\tau \varphi \rangle| = \begin{cases} 1 & \text{if } (\tau, w) = 0, \\ \leq \frac{2}{\sqrt{p}} & \text{if } (\tau, w) \neq 0. \end{cases} \quad (\text{I-.1})$$

- 2) *Crosscorrelation (cross-ambiguity function)*. For every  $\phi \neq \varphi \in \mathfrak{S}_O$  we have

$$|\langle \phi, M_w L_\tau \varphi \rangle| \leq \frac{4}{\sqrt{p}}, \quad (\text{I-.2})$$

for every  $\tau, w \in \mathbb{F}_p$ .

- 3) *Supremum*. For every signal  $\varphi \in \mathfrak{S}_O$  we have

$$\max \{|\varphi(t)| : t \in \mathbb{F}_p\} \leq \frac{2}{\sqrt{p}}.$$

- 4) *Fourier invariance*. For every signal  $\varphi \in \mathfrak{S}_O$  its Fourier transform  $\hat{\varphi}$  is (up to multiplication by a unitary scalar) also in  $\mathfrak{S}_O$ .

**Remark I-1:** Explicit algorithm that generates the oscillator system is given in Appendix B.

The oscillator system can be extended to a much larger system  $\mathfrak{S}_E$ , consisting of order of  $p^5$  signals if one is willing

S. Gurevich is with the Department of Mathematics, University of California, Berkeley, CA 94720, USA. Email: shamgar@math.berkeley.edu.

R. Hadani is with the Department of Mathematics, University of Chicago, IL 60637, USA. Email: hadani@math.uchicago.edu.

Nir Sochen is with the School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel. Email: sochen@post.tau.ac.il.

Manuscript received September, 2007.

to compromise Properties 1 and 2 for a weaker condition. The extended system consists of all signals of the form  $M_w L_\tau \varphi$  for  $\tau, w \in \mathbb{F}_p$  and  $\varphi \in \mathfrak{S}_O$ . It is not hard to show that  $\#(\mathfrak{S}_E) = p^2 \cdot \#(\mathfrak{S}_O) \approx p^5$ . As a consequence of (I-1) and (I-2) for every  $\varphi \neq \phi \in \mathfrak{S}_E$  we have

$$|\langle \varphi, \phi \rangle| \leq \frac{4}{\sqrt{p}}.$$

The characterization and construction of the oscillator system is representation theoretic and we devote the rest of the introduction to an intuitive explanation of the main underlying ideas. As a suggestive model example we explain first the construction of the well known system of chirp (Heisenberg) signals, deliberately taking a representation theoretic point of view (see [H2], [HCM] for a more comprehensive treatment).

#### A. Model example (Heisenberg system)

Let us denote by  $\psi : \mathbb{F}_p \rightarrow \mathbb{C}^\times$  the character  $\psi(t) = e^{\frac{2\pi i}{p} t}$ . We consider the pair of orthonormal bases  $\Delta = \{\delta_a : a \in \mathbb{F}_p\}$  and  $\Delta^\vee = \{\psi_a : a \in \mathbb{F}_p\}$ , where  $\psi_a(t) = \frac{1}{\sqrt{p}} \psi(at)$ , and  $\delta_a$  is the Kronecker delta function,  $\delta_a(t) = 1$  if  $t = a$  and  $\delta_a(t) = 0$  if  $t \neq a$ .

1) *Characterization of the bases  $\Delta$  and  $\Delta^\vee$ :* Let  $L : \mathcal{H} \rightarrow \mathcal{H}$  be the time shift operator  $L\varphi(t) = \varphi(t+1)$ . This operator is unitary and it induces a homomorphism of groups  $L : \mathbb{F}_p \rightarrow U(\mathcal{H})$  given by  $L_\tau \varphi(t) = \varphi(t+\tau)$  for any  $\tau \in \mathbb{F}_p$ .

Elements of the basis  $\Delta^\vee$  are character vectors with respect to the action  $L$ , i.e.,  $L_\tau \psi_a = \psi(a\tau) \psi_a$  for any  $\tau \in \mathbb{F}_p$ . In the same fashion, the basis  $\Delta$  consists of character vectors with respect to the homomorphism  $M : \mathbb{F}_p \rightarrow U(\mathcal{H})$  given by  $M_w \varphi(t) = \psi(wt) \varphi(t)$  for any  $w \in \mathbb{F}_p$ .

2) *The Heisenberg representation:* The homomorphisms  $L$  and  $M$  can be combined into a single map  $\tilde{\pi} : \mathbb{F}_p \times \mathbb{F}_p \rightarrow U(\mathcal{H})$  which sends a pair  $(\tau, w)$  to the unitary operator  $\tilde{\pi}(\tau, w) = \psi(-\frac{1}{2}\tau w) M_w \circ L_\tau$ . The plane  $\mathbb{F}_p \times \mathbb{F}_p$  is called the *time-frequency plane* and will be denoted by  $V$ . The map  $\tilde{\pi}$  is not an homomorphism since, in general, the operators  $L_\tau$  and  $M_w$  do not commute. This deficiency can be corrected if we consider the group  $H = V \times \mathbb{F}_p$  with multiplication given by

$$(\tau, w, z) \cdot (\tau', w', z') = (\tau + \tau', w + w', z + z' + \frac{1}{2}(\tau w' - \tau' w)).$$

The map  $\tilde{\pi}$  extends to a homomorphism  $\pi : H \rightarrow U(\mathcal{H})$  given by

$$\pi(\tau, w, z) = \psi(-\frac{1}{2}\tau w + z) M_w \circ L_\tau.$$

The group  $H$  is called the *Heisenberg group* and the homomorphism  $\pi$  is called the *Heisenberg representation*.

3) *Maximal commutative subgroups:* The Heisenberg group is no longer commutative, however, it contains various commutative subgroups which can be easily described. To every line  $L \subset V$ , that passes through the origin, one can associate a maximal commutative subgroup  $A_L = \{(l, 0) \in V \times \mathbb{F}_p : l \in L\}$ . It will be convenient to identify the subgroup  $A_L$  with the line  $L$ .

4) *Bases associated with lines:* Restricting the Heisenberg representation  $\pi$  to a subgroup  $L$  yields a decomposition of the Hilbert space  $\mathcal{H}$  into a direct sum of one-dimensional subspaces  $\mathcal{H} = \bigoplus \mathcal{H}_\chi$ , where  $\chi$  runs in the set  $L^\vee$  of (complex valued) characters of the group  $L$ . The subspace  $\mathcal{H}_\chi$  consists of vectors  $\varphi \in \mathcal{H}$  such that  $\pi(l)\varphi = \chi(l)\varphi$ . In other words, the space  $\mathcal{H}_\chi$  consists of common eigenvectors with respect to the commutative system of unitary operators  $\{\pi(l)\}_{l \in L}$  such that the operator  $\pi(l)$  has eigenvalue  $\chi(l)$ .

Choosing a unit vector  $\varphi_\chi \in \mathcal{H}_\chi$  for every  $\chi \in L^\vee$  we obtain an orthonormal basis  $\mathcal{B}_L = \{\varphi_\chi : \chi \in L^\vee\}$ . In particular,  $\Delta^\vee$  and  $\Delta$  are recovered as the bases associated with the lines  $T = \{(\tau, 0) : \tau \in \mathbb{F}_p\}$  and  $W = \{(0, w) : w \in \mathbb{F}_p\}$  respectively. For a general  $L$  the signals in  $\mathcal{B}_L$  are certain kind of chirps. Concluding, we associated with every line  $L \subset V$  an orthonormal basis  $\mathcal{B}_L$ , and overall we constructed a system of signals consisting of a union of orthonormal bases

$$\mathfrak{S}_H = \{\varphi \in \mathcal{B}_L : L \subset V\}.$$

For obvious reasons, the system  $\mathfrak{S}_H$  will be called the *Heisenberg system*.

5) *Properties of the Heisenberg system:* It will be convenient to introduce the following general notion. Given two signals  $\phi, \varphi \in \mathcal{H}$ , their matrix coefficient is the function  $m_{\phi, \varphi} : H \rightarrow \mathbb{C}$  given by  $m_{\phi, \varphi}(h) = \langle \phi, \pi(h)\varphi \rangle$ . In coordinates, if we write  $h = (\tau, w, z)$  then  $m_{\phi, \varphi}(h) = \psi(-\frac{1}{2}\tau w + z) \langle \phi, M_w \circ L_\tau \varphi \rangle$ . When  $\phi = \varphi$  the function  $m_{\phi, \varphi}$  is called the *ambiguity function* of the vector  $\varphi$  and is denoted by  $A_\varphi = m_{\varphi, \varphi}$ .

The system  $\mathfrak{S}_H$  consists of  $p+1$  orthonormal bases<sup>1</sup>, altogether  $p(p+1)$  signals and it satisfies the following properties [H2], [HCM]

1) *Autocorrelation.* For every signal  $\varphi \in \mathcal{B}_L$  the function  $|A_\varphi|$  is the characteristic function of the line  $L$ , i.e.,

$$|A_\varphi(v)| = \begin{cases} 0, & v \notin L, \\ 1, & v \in L. \end{cases}$$

2) *Crosscorrelation.* For every  $\phi \in \mathcal{B}_L$  and  $\varphi \in \mathcal{B}_M$  where  $L \neq M$  we have

$$|m_{\phi, \varphi}(v)| \leq \frac{1}{\sqrt{p}},$$

for every  $v \in V$ . If  $L = M$  then  $m_{\phi, \phi}$  is the characteristic function of some translation of the line  $L$ .

3) *Supremum.* A signal  $\varphi \in \mathfrak{S}_H$  is a unimodular function, i.e.,  $|\varphi(t)| = \frac{1}{\sqrt{p}}$  for every  $t \in \mathbb{F}_p$ , in particular we have

$$\max \{|\varphi(t)| : t \in \mathbb{F}_p\} = \frac{1}{\sqrt{p}} \ll 1.$$

*Remark I-A.1:* Note the main differences between the Heisenberg and the oscillator systems. The oscillator system consists of order of  $p^3$  signals, while the Heisenberg system consists of order of  $p^2$  signals. Signals in the oscillator system admits an ambiguity function concentrated at  $0 \in V$  (thumbtack pattern) while signals in the Heisenberg system admits ambiguity function concentrated on a line.

<sup>1</sup>Note that  $p+1$  is the number of lines in  $V$ .

### B. The oscillator system

Reflecting back on the Heisenberg system we see that each vector  $\varphi \in \mathfrak{S}_H$  is characterized in terms of action of the additive group  $G_a = \mathbb{F}_p$ . Roughly, in comparison, each vector in the oscillator system is characterized in terms of action of the multiplicative group  $G_m = \mathbb{F}_p^\times$ . Our next goal is to explain the last assertion. We begin by giving a model example.

Given a multiplicative character<sup>2</sup>  $\chi : G_m \rightarrow \mathbb{C}^\times$ , we define a vector  $\underline{\chi} \in \mathcal{H}$  by

$$\underline{\chi}(t) = \begin{cases} \frac{1}{\sqrt{p-1}}\chi(t), & t \neq 0, \\ 0, & t = 0. \end{cases}$$

We consider the system  $\mathcal{B}_{std} = \{\underline{\chi} : \chi \in G_m^\vee, \chi \neq 1\}$ , where  $G_m^\vee$  is the dual group of characters.

1) *Characterizing the system  $\mathcal{B}_{std}$ :* For each element  $a \in G_m$  let  $\rho_a : \mathcal{H} \rightarrow \mathcal{H}$  be the unitary operator acting by scaling  $\rho_a \varphi(t) = \varphi(at)$ . This collection of operators form a homomorphism  $\rho : G_m \rightarrow U(\mathcal{H})$ .

Elements of  $\mathcal{B}_{std}$  are character vectors with respect to  $\rho$ , i.e., the vector  $\underline{\chi}$  satisfies  $\rho_a(\underline{\chi}) = \chi(a)\underline{\chi}$  for every  $a \in G_m$ . In more conceptual terms, the action  $\rho$  yields a decomposition of the Hilbert space  $\mathcal{H}$  into character spaces  $\mathcal{H} = \bigoplus \mathcal{H}_\chi$ , where  $\chi$  runs in  $G_m^\vee$ . The system  $\mathcal{B}_{std}$  consists of a representative unit vector for each space  $\mathcal{H}_\chi$ ,  $\chi \neq 1$ .

2) *The Weil representation:* We would like to generalize the system  $\mathcal{B}_{std}$  in a similar fashion like we generalized the bases  $\Delta$  and  $\Delta^\vee$  in the Heisenberg setting. In order to do this we need to introduce several auxiliary operators.

Let  $\rho_a : \mathcal{H} \rightarrow \mathcal{H}$ ,  $a \in \mathbb{F}_p^\times$ , be the operators acting by  $\rho_a \varphi(t) = \sigma(a)\varphi(a^{-1}t)$  (scaling), where  $\sigma$  is the unique quadratic character of  $\mathbb{F}_p^\times$ , let  $\rho_T : \mathcal{H} \rightarrow \mathcal{H}$  be the operator acting by  $\rho_T \varphi(t) = \psi(t^2)\varphi(t)$  (quadratic modulation), and finally let  $\rho_S : \mathcal{H} \rightarrow \mathcal{H}$  be the operator of Fourier transform

$$\rho_S \varphi(t) = \frac{\nu}{\sqrt{p}} \sum_{s \in \mathbb{F}_p} \psi(ts) \varphi(s),$$

where  $\nu$  is a normalization constant which will be specified in the body of the paper. The operators  $\rho_a, \rho_T$  and  $\rho_S$  are unitary. Let us consider the subgroup of unitary operators generated by  $\rho_a, \rho_S$  and  $\rho_T$ . This group turns out to be isomorphic to the finite group  $Sp = SL_2(\mathbb{F}_p)$ , therefore we obtained a homomorphism  $\rho : Sp \rightarrow U(\mathcal{H})$ . The representation  $\rho$  is called the *Weil representation* [W] and it will play a prominent role in this paper.

3) *Systems associated with maximal (split) tori:* The group  $Sp$  consists of various types of commutative subgroups. We will be interested in maximal *diagonalizable* commutative subgroups. A subgroup of this type is called maximal *split torus*. The standard example is the subgroup consisting of all diagonal matrices

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in G_m \right\},$$

which is called the *standard torus*. The restriction of the Weil representation to a split torus  $T \subset Sp$  yields a decomposition

<sup>2</sup>A multiplicative character is a function  $\chi : G_m \rightarrow \mathbb{C}$  which satisfies  $\chi(xy) = \chi(x)\chi(y)$  for every  $x, y \in G_m$ .

of the Hilbert space  $\mathcal{H}$  into a direct sum of character spaces  $\mathcal{H} = \bigoplus \mathcal{H}_\chi$ , where  $\chi$  runs in the set of characters  $T^\vee$ . Choosing a unit vector  $\varphi_\chi \in \mathcal{H}_\chi$  for every  $\chi$  we obtain a collection of orthonormal vectors  $\mathcal{B}_T = \{\varphi_\chi : \chi \in T^\vee, \chi \neq \sigma\}$ . Overall, we constructed a system

$$\mathfrak{S}_O^s = \{\varphi \in \mathcal{B}_T : T \subset Sp \text{ split}\},$$

which will be referred to as the *split oscillator system*. We note that our initial system  $\mathcal{B}_{std}$  is recovered as  $\mathcal{B}_{std} = \mathcal{B}_A$ .

4) *Systems associated with maximal (non-split) tori:* From the point of view of this paper, the most interesting maximal commutative subgroups in  $Sp$  are those which are diagonalizable over an extension field rather than over the base field  $\mathbb{F}_p$ . A subgroup of this type is called maximal *non-split torus*. It might be suggestive to first explain the analogue notion in the more familiar setting of the field  $\mathbb{R}$ . Here, the standard example of a maximal non-split torus is the circle group  $SO(2) \subset SL_2(\mathbb{R})$ . Indeed, it is a maximal commutative subgroup which becomes diagonalizable when considered over the extension field  $\mathbb{C}$  of complex numbers.

The above analogy suggests a way to construct examples of maximal non-split tori in the finite field setting as well. Let us assume for simplicity that  $-1$  does not admit a square root in  $\mathbb{F}_p$ . The group  $Sp$  acts naturally on the plane  $V = \mathbb{F}_p \times \mathbb{F}_p$ . Consider the symmetric bilinear form  $B$  on  $V$  given by

$$B((t, w), (t', w')) = tt' + ww'.$$

An example of maximal non-split torus is the subgroup  $T_{ns} \subset Sp$  consisting of all elements  $g \in Sp$  preserving the form  $B$ , i.e.,  $g \in T_{ns}$  if and only if  $B(gu, gv) = B(u, v)$  for every  $u, v \in V$ . In the same fashion like in the split case, restricting the Weil representation to a non-split torus  $T$  yields a decomposition into character spaces  $\mathcal{H} = \bigoplus \mathcal{H}_\chi$ . Choosing a unit vector  $\varphi_\chi \in \mathcal{H}_\chi$  for every  $\chi \in T^\vee$  we obtain an orthonormal basis  $\mathcal{B}_T$ . Overall, we constructed a system of signals

$$\mathfrak{S}_O^{ns} = \{\varphi \in \mathcal{B}_T : T \subset Sp \text{ non-split}\}.$$

The system  $\mathfrak{S}_O^{ns}$  will be referred to as the *non-split oscillator system*. The construction of the system  $\mathfrak{S}_O^{ns}$  and the techniques used to study its properties are the main contribution of this paper.

5) *Behavior under Fourier transform:* The oscillator system is closed under the operation of Fourier transform, i.e., for every  $\varphi \in \mathfrak{S}_O$  we have that (up to multiplication by a unitary scalar)  $\widehat{\varphi} \in \mathfrak{S}_O$ . The Fourier transform on the space  $\mathbb{C}(\mathbb{F}_p)$  appears as a specific operator  $\rho(w)$  in the Weil representation, where

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in Sp.$$

Given a signal  $\varphi \in \mathcal{B}_T \subset \mathfrak{S}_O$ , its Fourier transform  $\widehat{\varphi} = \rho(w)\varphi$  is (up to multiplication by a unitary scalar) a signal in  $\mathcal{B}_{T'}$  where  $T' = wTw^{-1}$ . In fact,  $\mathfrak{S}_O$  is closed under all the operators in the Weil representation! Given an element  $g \in Sp$  and a signal  $\varphi \in \mathcal{B}_T$  we have, up to a unitary scalar, that  $\rho(g)\varphi \in \mathcal{B}_{T'}$ , where  $T' = gTg^{-1}$ .

In addition, the Weyl element  $w$  is an element in some maximal torus  $T_w$  (the split type of  $T_w$  depends on the

characteristic  $p$  of the field) and as a result signals  $\varphi \in \mathcal{B}_{T_w}$  are, in particular, eigenvectors of the Fourier transform. As a consequence a signal  $\varphi \in \mathcal{B}_{T_w}$  and its Fourier transform  $\hat{\varphi}$  differ by a unitary constant, therefore are practically the "same" for all essential matters.

These properties might be relevant for applications to OFDM (Orthogonal Frequency Division Multiplexing) [C] where one requires good properties both from the signal and its Fourier transform.

6) *Relation to the harmonic oscillator*: Here we give the explanation why functions in the non-split oscillator system  $\mathfrak{S}_O^{ns}$  constitute a finite analogue of the eigenfunctions of the harmonic oscillator in the real setting. The Weil representation establishes the dictionary between these two, seemingly, unrelated objects. The argument works as follows.

The one-dimensional harmonic oscillator is given by the differential operator  $D = \partial^2 - t^2$ . The operator  $D$  can be exponentiated to give a unitary representation of the circle group  $\rho : SO(2, \mathbb{R}) \rightarrow U(\mathcal{H})$  where  $\rho(t) = e^{itD}$ . Eigenfunctions of  $D$  are naturally identified with character vectors with respect to  $\rho$ . The crucial point is that  $\rho$  is the restriction of the Weil representation of  $SL_2(\mathbb{R})$  to the maximal non-split torus  $SO(2, \mathbb{R}) \subset SL_2(\mathbb{R})$ .

Summarizing, the eigenfunctions of the harmonic oscillator and functions in  $\mathfrak{S}_O^{ns}$  are governed by the same mechanism, namely both are character vectors with respect to the restriction of the Weil representation to a maximal non-split torus in  $SL_2$ . The only difference appears to be the field of definition, which for the harmonic oscillator is the reals and for the oscillator functions is the finite field.

### C. Applications

Two applications of the oscillator system will be described. The first application is to the theory of discrete radar. The second application is to CDMA systems. We will give a brief explanation of these problems, while emphasizing the relation to the Heisenberg representation.

1) *Discrete Radar*: The theory of discrete radar is closely related [HCM] to the finite Heisenberg group  $H$ . A radar sends a signal  $\varphi(t)$  and obtains an echo  $e(t)$ . The goal [Wo] is to reconstruct, in maximal accuracy, the target range and velocity. The signal  $\varphi(t)$  and the echo  $e(t)$  are, principally, related by the transformation

$$e(t) = e^{2\pi i w t} \varphi(t + \tau) = M_w L_\tau \varphi(t),$$

where the time shift  $\tau$  encodes the distance of the target from the radar and the phase shift encodes the velocity of the target. Equivalently saying, the transmitted signal  $\varphi$  and the received echo  $e$  are related by an action of an element  $h_0 \in H$ , i.e.,  $e = \pi(h_0)\varphi$ . The problem of discrete radar can be described as follows. Given a signal  $\varphi$  and an echo  $e = \pi(h_0)\varphi$  extract the value of  $h_0$ .

It is easy to show that  $|m_{\varphi, e}(h)| = |A_\varphi(h \cdot h_0)|$  and it obtains its maximum at  $h_0^{-1}$ . This suggests that a desired signal  $\varphi$  for discrete radar should admit an ambiguity function  $A_\varphi$  which is highly concentrated around  $0 \in H$ , which is a property satisfied by signals in the oscillator system (Property 2).

*Remark I-C.1*: It should be noted that the system  $\mathfrak{S}_O$  is "large" consisting of approximately  $p^3$  signals. This property becomes important in a *jamming* scenario.

2) *Code Division Multiple Access (CDMA)*: We are considering the following setting.

- There exists a collection of users  $i \in I$ , each holding a *bit* of information  $b_i \in \mathbb{C}$  (usually  $b_i$  is taken to be an  $N$ 'th root of unity).
- Each user transmits his bit of information, say, to a central antenna. In order to do that, he multiplies his bit  $b_i$  by a private signal  $\varphi_i \in \mathcal{H}$  and forms a message  $u_i = b_i \varphi_i$ .
- The transmission is carried through a single channel (for example in the case of cellular communication the channel is the atmosphere), therefore the message received by the antenna is the sum

$$u = \sum_i u_i.$$

The main problem [V] is to extract the individual bits  $b_i$  from the message  $u$ . The bit  $b_i$  can be estimated by calculating the inner product

$$\langle \varphi_i, u \rangle = \sum_i \langle \varphi_i, u_j \rangle = \sum_j b_j \langle \varphi_i, \varphi_j \rangle = b_i + \sum_{j \neq i} b_j \langle \varphi_i, \varphi_j \rangle.$$

The last expression above should be considered as a sum of the information bit  $b_i$  and an additional noise caused by the interference of the other messages. This is the standard scenario also called the *Synchronous* scenario. In practice, more complicated scenarios appear, e.g., *asynchronous scenario* - in which each message  $u_i$  is allowed to acquire an arbitrary time shift  $u_i(t) \mapsto u_i(t + \tau_i)$ , *phase shift scenario* - in which each message  $u_i$  is allowed to acquire an arbitrary phase shift  $u_i(t) \mapsto e^{\frac{2\pi i}{p} w_i t} u_i(t)$  and probably also a combination of the two where each message  $u_i$  is allowed to acquire an arbitrary distortion of the form  $u_i(t) \mapsto e^{\frac{2\pi i}{p} w_i t} u_i(t + \tau_i)$ .

The previous discussion suggests that what we are seeking for is a large system  $\mathfrak{S}$  of signals which will enable a reliable extraction of each bit  $b_i$  for as many users transmitting through the channel simultaneously.

*Definition I-C.2 (Stability conditions)*: Two unit signals  $\phi \neq \varphi$  are called **stably cross-correlated** if  $|m_{\varphi, \phi}(v)| \ll 1$  for every  $v \in V$ . A unit signal  $\varphi$  is called **stably auto-correlated** if  $|A_\varphi(v)| \ll 1$ , for every  $v \neq 0$ . A system  $\mathfrak{S}$  of signals is called a **stable** system if every signal  $\varphi \in \mathfrak{S}$  is stably auto-correlated and any two different signals  $\phi, \varphi \in \mathfrak{S}$  are stably cross-correlated.

Formally what we require for CDMA is a stable system  $\mathfrak{S}$ . Let us explain why this corresponds to a reasonable solution to our problem. At a certain time  $t$  the antenna receives a message

$$u = \sum_{i \in J} u_i,$$

which is transmitted from a subset of users  $J \subset I$ . Each message  $u_i$ ,  $i \in J$ , is of the form  $u_i = b_i e^{\frac{2\pi i}{p} w_i t} \varphi_i(t + \tau_i) = b_i \pi(h_i) \varphi_i$ , where  $h_i \in H$ . In order to extract the bit  $b_i$  we compute the matrix coefficient

$$m_{\varphi_i, u} = b_i R_{h_i} A_{\varphi_i} + \#(J - \{i\})o(1),$$

where  $R_{h_i}$  is the operator of right translation  $R_{h_i}A_{\varphi_i}(h) = A_{\varphi_i}(hh_i)$ .

If the cardinality of the set  $J$  is not too big then by evaluating  $m_{\varphi_i, u}$  at  $h = h_i^{-1}$  we can reconstruct the bit  $b_i$ . It follows from (I-1) and (I-2) that the oscillator system  $\mathfrak{S}_O$  can support order of  $p^3$  users, enabling reliable reconstruction when order of  $\sqrt{p}$  users are transmitting simultaneously.

#### D. Structure of the paper

Apart from the introduction, the paper consists of three sections and two appendices. In Section II several basic notions from representation theory are introduced. Particularly, we define the Heisenberg and Weil representations over finite fields. In addition, we spend some space explaining the Weyl transform which is a key tool in our approach to the Heisenberg and Weil representations. In Section III the geometric counterpart of the Weil representation is established, in particular, we explain the geometric Weyl transform. In Section IV we introduce the oscillator functions and then their main properties are stated in a series of propositions. Finally, we explain the main ideas in the proof of each proposition. In Appendix A we give the proofs of all technical statements which appear in the body of the paper. Finally, in Appendix B we describe an explicit algorithm that generates the oscillator system  $\mathfrak{S}_O^s$  associated with the collection of split tori.

#### E. Remark about field extensions

All the results in the introduction were stated for the basic finite field  $\mathbb{F}_p$ , where  $p$  is an odd prime, for the reason of making the terminology more accessible. However, in the body of the paper, all the results are stated and proved for any field extension of the form  $\mathbb{F}_q$  with  $q = p^n$ .

## II. PRELIMINARIES FROM REPRESENTATION THEORY

In this section several fundamental notions from representation theory are explained. Let  $\mathbb{F}_q$  denote the finite field consisting of  $q$  elements, where  $q$  is odd.

#### A. The Heisenberg group

Let  $(V, \omega)$  be a two-dimensional symplectic vector space over  $\mathbb{F}_q$ . Considering  $V$  as an abelian group, it admits a non-trivial central extension

$$0 \rightarrow \mathbb{F}_q \rightarrow H \rightarrow V \rightarrow 0,$$

called the *Heisenberg group*. Concretely, the group  $H$  can be presented as the set  $H = V \times \mathbb{F}_q$  with the multiplication given by

$$(v, z) \cdot (v', z') = (v + v', z + z' + \frac{1}{2}\omega(v, v')).$$

The center of  $H$  is  $Z = Z(H) = \{(0, z) : z \in \mathbb{F}_q\}$ . The symplectic group  $Sp = Sp(V, \omega)$  acts by automorphism of  $H$  through its action on the  $V$ -coordinate.

#### B. The Heisenberg representation

One of the most important attributes of the group  $H$  is that it admits, principally, a unique irreducible representation. The precise statement is the content of the following celebrated theorem.

*Theorem II-B.1 (Stone-von Neuman):* Let  $\psi : Z \rightarrow \mathbb{C}^\times$  be a non-trivial character of the center. There exists a unique (up to isomorphism) irreducible unitary representation  $(\pi, H, \mathcal{H})$  with the center acting by  $\psi$ , i.e.,  $\pi|_Z = \psi \cdot Id_{\mathcal{H}}$ .

The representation  $\pi$  which appears in the above theorem will be called the *Heisenberg representation*.

1) *Schrödinger Models:* The Heisenberg representation admits various different models (realizations). These models appear in families. In this paper we will be interested in a specific family associated with *Lagrangian splittings*. These models are usually referred to in the literature as *Schrödinger models*. Let us explain how these models are constructed.

*Definition II-B.2:* A Lagrangian splitting  $S$  of  $V$  is a pair  $(L, M)$  of Lagrangian subspaces<sup>3</sup> such that  $L \cap M = 0$ .

Given a Lagrangian splitting  $S = (L, M)$  there exists a model  $(\pi_S, H, \mathcal{H}_S)$ , where the Hilbert space  $\mathcal{H}_S$  is  $\mathbb{C}(L)$  and the action  $\pi_S$  is given by the following formulas  $\pi_S(l) = L_l$ ,  $\pi_S(m) = M_{\psi(\omega(\cdot, m))}$  and  $\pi_S(z) = M_{\psi(z)}$ . Finally, the Hermitian product is given by  $\langle f, g \rangle = \sum_{x \in L} f(x)\overline{g(x)}$  for  $f, g \in \mathcal{H}_S$ .

#### C. The Weyl transform

We see from the previous paragraph that the Hilbert space of the Heisenberg representation can be identified with the Hilbert space of complex valued functions on  $\mathbb{F}_q$ . This fact has far reaching implications, in particular, it enables to study properties of functions in representation theoretic terms. An important tool for doing that is the Weyl transform [We2] which is principally equivalent to the operation of taking matrix coefficient. Given a linear operator  $A : \mathcal{H} \rightarrow \mathcal{H}$  we can associate to it a function on the group  $H$  defined as follows

$$W_A(h) = \frac{1}{\dim \mathcal{H}} \text{Tr}(A\pi(h^{-1})).$$

The transform  $W : \text{End}(\mathcal{H}) \rightarrow \mathbb{C}(H)$  is called the *Weyl transform* [H1].

1) *Properties of the Weyl transform:* The image of the Weyl transform is the space  $\mathbb{C}(H, \psi^{-1})$  consisting of functions  $f \in \mathbb{C}(H)$  such that  $f(z \cdot h) = \psi^{-1}(z)f(h)$  for every  $z \in Z$ . Moreover, it admits a left inverse  $\Pi : \mathbb{C}(H) \rightarrow \text{End}(\mathcal{H})$  given by  $\Pi(f) = \frac{1}{q} \sum_{h \in H} f(h)\pi(h)$ . The transforms  $W$  and  $\Pi$  are morphisms of  $H \times H$ -representations, i.e., if we denote by  $L, R : H \rightarrow \text{End}(\mathbb{C}(H))$  the left and right regular representations of  $H$  then  $W_{\pi(h_1)A\pi(h_2)} = R_{h_2^{-1}}L_{h_1}W_A$ . Finally, the transforms  $W$  and  $\Pi$  exchange composition of operators  $\circ$  with group theoretic convolution  $*$ , i.e.,  $W_{A \circ B} = W_A * W_B$  for every  $A, B \in \text{End}(\mathcal{H})$ , where we take

$$W_A * W_B(h) = \frac{1}{q} \sum_{h_1 \cdot h_2 = h} W_A(h_1)W_B(h_2).$$

<sup>3</sup>We remind the reader that a Lagrangian subspace  $L \subset V$  is maximal subspace on which the symplectic form vanishes.

It will be sometimes convenient to identify  $\mathbb{C}(H, \psi^{-1})$  with  $\mathbb{C}(V)$ . Under this identification  $\Pi$  is given by  $\Pi(f) = \sum_{v \in V} f(v) \pi(v)$  and

$$W_A * W_B(v) = \sum_{v_1 + v_2 = v} \psi\left(-\frac{1}{2}\omega(v_1, v_2)\right) W_A(v_1) W_B(v_2). \quad (\text{II-C.1})$$

2) *Explicit formulas:* Given a Schrödinger model  $(\pi_S, H, \mathcal{H}_S)$  associated to a Lagrangian splitting  $S = (L, M)$ , every operator  $A \in \text{End}(\mathcal{H}_S)$  can be presented as a function on  $L \times L$ . In this presentation, composition is given by convolution of functions  $f \circ g(x, y) = \sum_{z \in L} f(x, z) g(z, y)$ . If we identify  $\mathbb{C}(H, \psi^{-1})$  with  $\mathbb{C}(L \times M)$  then the transforms  $W$  and  $\Pi$  are realized as

$$\begin{aligned} W_S &: \mathbb{C}(L \times L) \rightarrow \mathbb{C}(L \times M), \\ \Pi_S &: \mathbb{C}(L \times M) \rightarrow \mathbb{C}(L \times L), \end{aligned}$$

and are given by  $W_S = F_{M,L} \circ \alpha^*$  and  $\Pi_S = \beta^* \circ F_{M,L}^{-1}$ . Here,  $\alpha^*, \beta^*$  are pullbacks via the maps  $\alpha, \beta = \alpha^{-1} : L \times L \rightarrow L \times L$  with  $\alpha(x, y) = (\frac{y-x}{2}, \frac{x+y}{2})$  and  $\beta(x, y) = (y-x, x+y)$  and  $F_{M,L} : \mathbb{C}(L \times L) \rightarrow \mathbb{C}(L \times M)$  is the Fourier transform along the right  $L$ -coordinate

$$F_{M,L}(f)(l, m) = \frac{1}{\dim \mathcal{H}} \sum_{x \in L} \psi\left(\frac{1}{2}\omega(m, x)\right) f(l, x).$$

#### D. Intertwining maps

Given a pair of Lagrangian splittings  $S_i = (L_i, M_i)$ ,  $i = 1, 2$ , let us denote by  $F_{2,1} = F_{S_2, S_1}$  the composition  $\Pi_{S_2} \circ W_{S_1}$ . The map  $F_{2,1}$  is a morphism of  $H \times H$ -representations and will be called *intertwining map*. The map  $F_{2,1}$  splits into a tensor product  $F_{2,1} = F^L \boxtimes F^R$  where the specific form of  $F^L$  and  $F^R$  depends on the relative position of the two splittings. We will describe  $F^L$  and  $F^R$  explicitly. Let us denote by  $A$  the tautological isomorphism  $L_2 \times M_2 \xrightarrow{\sim} L_1 \times M_1$ . The specific form of  $F^L$  and  $F^R$  depends on the value of  $A_{21}$ . For every function  $f \in \mathbb{C}(L_1)$

- If  $A_{21} \neq 0$  then

$$\begin{aligned} F^L(f)(x) &= \frac{1}{\dim \mathcal{H}} \sum_{y \in L_1} \psi\left(\frac{1}{2}\omega(Dx, x) + \omega(Bx - Cy, y)\right) f(y), \\ F^R(f)(x) &= \frac{1}{\dim \mathcal{H}} \sum_{y \in L_1} \psi\left(\omega(Cy - Bx, y) - \frac{1}{2}\omega(Dx, x)\right) f(y), \end{aligned}$$

where  $B = A_{12} - A_{11}A_{21}^{-1}A_{22}$ ,  $C = A_{11}A_{21}^{-1}$  and  $D = A_{21}^{-1}A_{22}$ .

- If  $A_{21} = 0$  then

$$\begin{aligned} F^L(f)(x) &= \psi\left(\frac{1}{2}\omega(x, A_{11}x)\right) f(A_{11}x), \\ F^R(f)(x) &= \psi\left(-\frac{1}{2}\omega(x, A_{11}x)\right) f(A_{11}x). \end{aligned}$$

#### E. The Weil representation

A direct consequence of Theorem II-B.1 is the existence of a projective representation  $\tilde{\rho} : Sp \rightarrow PGL(\mathcal{H})$ . The classical construction of  $\tilde{\rho}$  out of the Heisenberg representation  $\pi$  is due to Weil [W]. Considering the Heisenberg representation  $\pi$  and an element  $g \in Sp$ , one can define a new representation  $\pi^g$  acting on the same Hilbert space via  $\pi^g(h) =$

$\pi(g(h))$ . Clearly both  $\pi$  and  $\pi^g$  have central character  $\psi$  hence by Theorem II-B.1 they are isomorphic. Since the space  $\text{Hom}_H(\pi, \pi^g)$  is one-dimensional, choosing for every  $g \in Sp$  a non-zero representative  $\tilde{\rho}(g) \in \text{Hom}_H(\pi, \pi^g)$  gives the required projective representation. In more concrete terms, the projective representation  $\tilde{\rho}$  is characterized by the formula

$$\tilde{\rho}(g) \pi(h) \tilde{\rho}(g^{-1}) = \pi(g(h)), \quad (\text{II-E.1})$$

for every  $g \in Sp$  and  $h \in H$ . It is a peculiar phenomenon of the finite field setting that the projective representation  $\tilde{\rho}$  can be linearized into an honest representation

*Theorem II-E.1:* There exists a unique<sup>4</sup> unitary representation

$$\rho : Sp \longrightarrow GL(\mathcal{H}),$$

satisfying the formula (II-E.1).

1) *Weil representation (invariant presentation):* An elegant description of the Weil representation can be obtained using the Weyl transform [GH1]. Given an element  $g \in Sp$ , the operator  $\rho(g)$  can be written as  $\rho(g) = \pi(K_g)$ , where  $K_g$  is the Weyl transform  $K_g = W_{\rho(g)}$ . The collection of functions  $\{K_g\}_{g \in Sp}$  form a single function  $K : Sp \times H \rightarrow \mathbb{C}$ . The multiplicativity property of  $\rho$  is manifested as

$$K_g * K_h = K_{gh} \quad \text{for every } g, h \in Sp. \quad (\text{II-E.2})$$

These relations can be written as a single relation satisfied by the function  $K$ . Consider the maps  $m : Sp \times Sp \times V \rightarrow Sp \times V$  and  $p_i : Sp \times Sp \times V \rightarrow Sp \times V$ ,  $i = 1, 2$ . Here  $m$  is the multiplication map  $m(g_1, g_2, v) = (g_1 \cdot g_2, v)$  and  $p_i(g_1, g_2, v) = (g_i, v)$ ,  $i = 1, 2$ . The multiplicativity relations (II-E.2) are equivalent to

$$m^* K = p_1^* K * p_2^* K.$$

Finally, the function  $K$  can be explicitly described [GH1] on an appropriate subset of  $Sp$ . Let  $U \subset Sp$  denote the subset consisting of all elements  $g \in Sp$  such that  $g - I$  is invertible. For every  $g \in U$  and  $v \in V$  we have

$$K(g, v) = \frac{1}{\dim \mathcal{H}} \mu(g) \psi\left(\frac{1}{4}\omega(\kappa(g)v, v)\right), \quad (\text{II-E.3})$$

where  $\kappa(g) = \frac{g+I}{g-I}$  is the Cayley transform [H1], [We1],  $\mu(g) = \sigma(-\det(\kappa(g) + I))$  and  $\sigma$  is the unique quadratic character of the multiplicative group  $\mathbb{F}_q^\times$ .

### III. GEOMETRIC REPRESENTATION THEORY

In this section a geometric counterpart of the Heisenberg and the Weil representations will be established. The approach we employ is called *geometrization*, by which sets are replaced by algebraic varieties (over the finite field) and functions are replaced by  $\ell$ -adic Weil sheaves. Informally, algebraic varieties might be thought of as smooth manifolds and sheaves as vector bundles. Formally, this way of thinking is far from the true mathematical definition of these "beasts", but still it gives a good intuitive idea of what is evolving.

<sup>4</sup>Unique, except in the case the finite field is  $\mathbb{F}_3$  and  $\dim V = 2$ . For the canonical choice in the latter case see [GH1].

### A. Preliminaries from algebraic geometry

We denote by  $k$  an algebraic closure of the finite field  $\mathbb{F}_q$ .

1) *Varieties*: In this paper, a variety means a smooth quasi projective algebraic variety over  $k$ . A variety over  $\mathbb{F}_q$  is a variety  $\mathbf{X}$  equipped with an endomorphism  $Fr : \mathbf{X} \rightarrow \mathbf{X}$  called Frobenius. We denote by  $X$  the set of points which are fixed by Frobenius, i.e.,  $X = \{x \in \mathbf{X} : Fr(x) = x\}$ .

2) *Sheaves*: We denote by  $D(\mathbf{X})$  the bounded derived category of constructible  $\ell$ -adic sheaves on  $\mathbf{X}$  [BBD] and by  $D^{p,0} = D^{p,\geq 0} \cap D^{p,\leq 0}$  the Abelian category of perverse sheaves on the variety  $\mathbf{X}$ . An object  $\mathcal{F} \in D^{p,n}$  is called  $[n]$ -perverse. Note that  $\mathcal{F}$  is  $[n]$ -perverse if and only if  $\mathcal{F}[n] \in D^{p,0}$ , where  $[\cdot]$  denotes the standard cohomological shift functor. A Weil structure on a sheaf  $\mathcal{F} \in D(\mathbf{X})$  is an isomorphism  $\theta : \mathcal{F} \xrightarrow{\sim} Fr^* \mathcal{F}$ . A pair  $(\mathcal{F}, \theta)$  is called a Weil sheaf. By an abuse of notation we often denote  $\theta$  also by  $Fr$ .

**Assumption:** We choose once an identification  $\overline{\mathbb{Q}}_\ell \simeq \mathbb{C}$ , hence all sheaves are considered over the complex numbers.

3) *Sheaf to function correspondence*: Given a Weil sheaf  $\mathcal{F}$  on  $\mathbf{X}$  we can associate to it a function  $f^\mathcal{F} : X \rightarrow \mathbb{C}$  by

$$f^\mathcal{F}(x) = \chi_{Fr}(\mathcal{F}|_x) = \sum_i (-1)^i Tr(Fr|_{H^i(\mathcal{F}_x)}).$$

This procedure is called *Grothendieck's sheaf-to-function correspondence* [G], [Ga]. It interchanges the functors of pull-back, integration with compact support and tensor product with pull-back of functions, summation along the fibers and multiplication of functions respectively.

4) *Sheaves on one-dimensional varieties*: Let  $\mathbf{X}$  be an one-dimensional variety.

**Elementary sheaves.** An elementary sheaf  $\mathcal{F}$  on  $\mathbf{X}$  is an object in  $D(\mathbf{X})$  which is concentrated at a single degree with no punctual sections [K]. We will denote by  $\mathcal{F}(t)$ ,  $t \in \mathbf{X}$ , the restriction of  $\mathcal{F}$  to a punctured Henselian neighborhood of  $t$ . Alternatively, if we think of  $\mathcal{F}$  as a representation of  $G = Gal(E/F)$ , where  $E$  is some separable Galois extension of the fraction field of  $\mathbf{X}$  then  $\mathcal{F}(t)$  is the restriction of  $\mathcal{F}$  to the inertia subgroup  $I_t \subset G$ .

**Artin-Schreier sheaf.** We denote by  $\mathcal{L}_\psi$  the Artin-Schreier sheaf [Ga] on the variety  $\mathbb{G}_a$  which is associated to an additive character  $\psi : \mathbb{F}_q \rightarrow \mathbb{C}^\times$ , in particular we have  $f^{\mathcal{L}_\psi} = \psi$ .

**Kummer sheaf.** We denote by  $\mathcal{L}_\chi$  the Kummer sheaf on the variety  $\mathbb{G}_m$  which is associated to a multiplicative character  $\chi : \mathbb{F}_q^\times \rightarrow \mathbb{C}^\times$ , in particular  $f^{\mathcal{L}_\chi} = \chi$ .

### B. The geometric Weyl transform

We use the notations of Subsection II-C. Here we take  $(V, \omega)$  to be a dimensional symplectic vector space in the category of algebraic varieties over  $\mathbb{F}_q$ . Given a Lagrangian splitting  $\mathbf{S} = (\mathbf{L}, \mathbf{M})$  of  $\mathbf{V}$  we think of the category  $D(\mathbf{L} \times \mathbf{L})$  as a geometric counterpart for the vector space of operators  $\text{End}(\mathcal{H}_S)$ . In particular, given a pair of sheaves  $\mathcal{F}, \mathcal{G} \in D(\mathbf{L} \times \mathbf{L})$  their convolution is defined by

$$\mathcal{F} \circ \mathcal{G} = \int_{z \in \mathbf{L}} \mathcal{F}(x, z) \otimes \mathcal{G}(z, y). \quad (\text{III-B.1})$$

where  $\int$  denotes the functor of integration with compact support. The geometric Weyl transform is a functor  $W_S : D(\mathbf{L} \times \mathbf{L}) \rightarrow D(\mathbf{L} \times \mathbf{M})$  given by  $W_S = F_{\mathbf{M}, \mathbf{L}} \circ \alpha^*[2]$ . Here  $F_{\mathbf{M}, \mathbf{L}}$  is the  $\ell$ -adic Fourier transform along the right  $\mathbf{L}$ -coordinate

$$F_{\mathbf{M}, \mathbf{L}}(\mathcal{F})(l, m) = \int_{x \in \mathbf{L}} \mathcal{L}_\psi\left(\frac{1}{2}\omega(m, x)\right) \otimes \mathcal{F}(l, x).$$

1) *Properties of the geometric Weyl transform*: The functor  $W_S$  admits an inverse functor  $\Pi_S$ , which is given by  $\Pi_S = \beta^* \circ F_{\mathbf{M}, \mathbf{L}}^{-1}$ , with  $\beta = \alpha^{-1}$ . In addition, the functors  $W_S$  and  $\Pi_S$  interchange between matrix convolution  $\circ$  and group theoretic convolution  $*$ , i.e., there exists natural isomorphisms

$$\begin{aligned} W_S(\mathcal{F} \circ \mathcal{G}) &\simeq W_S(\mathcal{F}) * W_S(\mathcal{G}), \\ \Pi_S(\mathcal{F} * \mathcal{G}) &\simeq \Pi_S(\mathcal{F}) \circ \Pi_S(\mathcal{G}). \end{aligned}$$

Here

$$W_S(\mathcal{F}) * W_S(\mathcal{G})(v) =$$

$$\int_{v_1 + v_2 = v} \mathcal{L}_\psi\left(-\frac{1}{2}\omega(v_1, v_2)\right) \otimes W_S(\mathcal{F})(v_1) \otimes W_S(\mathcal{G})(v_2).$$

Finally,  $W_S$  and  $\Pi_S$  are compatible with perverse  $t$ -structure, more precisely  $W_S$  and  $\Pi_S$  shift the perversity degree by  $-1$  and  $1$  respectively.

### C. Intertwining functors

Given a pair of Lagrangian splittings  $\mathbf{S}_i = (\mathbf{L}_i, \mathbf{M}_i)$ ,  $i = 1, 2$ , the intertwining functor  $F_{\mathbf{S}_2, \mathbf{S}_1}$  is the composition of functors  $t_{\mathbf{S}_2} \circ W_{\mathbf{S}_1}$ . The functor  $F_{\mathbf{S}_2, \mathbf{S}_1}$  establishes an equivalence between the categories  $D(\mathbf{L}_1 \times \mathbf{L}_1)$  and  $D(\mathbf{L}_2 \times \mathbf{L}_2)$ , it commutes with convolution and sends  $D^{p,0}(\mathbf{L}_1 \times \mathbf{L}_1)$  to  $D^{p,0}(\mathbf{L}_2 \times \mathbf{L}_2)$ . These properties directly follow from the properties of the functors  $W_S$  and  $\Pi_S$ . Finally, we have  $F_{\mathbf{S}_2, \mathbf{S}_1} = F^L \boxtimes F^R$  and:

- If  $A_{21} \neq 0$  then

$$\begin{aligned} F^L(\mathcal{G})(x) &= \int_{y \in \mathbf{L}_1} \mathcal{L}_\psi\left[\frac{1}{2}\omega(Dx, x) + \omega(Bx, y) + \frac{1}{2}\omega(y, Cy)\right] \otimes \mathcal{G}(y)[1], \\ F^R(\mathcal{G})(x) &= \int_{y \in \mathbf{L}_1} \mathcal{L}_\psi\left[-\frac{1}{2}\omega(Dx, x) - \omega(Bx, y) - \frac{1}{2}\omega(y, Cy)\right] \otimes \mathcal{G}(y)[1], \end{aligned}$$

with  $B, C$  and  $D$  given by the same formulas as in subsection II-D.

- If  $A_{21} = 0$  then

$$\begin{aligned} F^L(\mathcal{G})(x) &= \mathcal{L}_\psi\left(\frac{1}{2}\omega(x, A_{11}x)\right) \otimes \mathcal{G}(A_{11}x), \\ F^R(\mathcal{G})(x) &= \mathcal{L}_\psi\left(-\frac{1}{2}\omega(x, A_{11}x)\right) \otimes \mathcal{G}(A_{11}x). \end{aligned}$$

### D. Geometric Weil representation

We conclude this section by recalling the main result of [GH1] regarding the existence of a sheaf theoretic counterpart of the Weil representation. We use the notations from Subsection II-E.

**Theorem III-D.1:** There exists a geometrically irreducible  $[\dim \mathbf{Sp}]$ -perverse Weil sheaf  $\mathcal{K}$  of pure weight zero on  $\mathbf{Sp} \times \mathbf{V}$  satisfying the following properties

- 1) **Multiplicativity.** There exists an isomorphism  $m^* \mathcal{K} \simeq p_1^* \mathcal{K} * p_2^* \mathcal{K}$ .
- 2) **Function.** We have  $f^{\mathcal{K}} = K$ .
- 3) **Formula.** For every  $g \in \mathbf{U}$  we have

$$\mathcal{K}(g, v) = \mathcal{L}_\mu(g) \otimes \mathcal{L}_\psi \left( \frac{1}{4} \omega(\kappa(g)v, v) \right) [2](1),$$

where  $\mathcal{L}_\mu(g) = \mathcal{L}_\sigma(-\det(\kappa(g) + I))$ .

#### IV. OSCILLATOR FUNCTIONS

##### A. The theory of tori

There exists two conjugacy classes of (rational points of algebraic) tori in  $Sp \simeq SL_2(\mathbb{F}_q)$ . The first system consists of those tori which are conjugated to the standard diagonal torus

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^\times \right\}.$$

A torus in this class is called a *split* torus. The second class consists of those tori which are not conjugated to  $A$ . A torus in this class is called a *non-split* torus (sometimes it is called inert torus). All split (non-split) tori are conjugated to one another. The number of split (non-split) tori is  $\#(Sp/N_s) = \frac{q(q+1)}{2}$  ( $\#(Sp/N_{ns}) = q(q-1)$ ), where  $N_s$  ( $N_{ns}$ ) is the normalizer group of some split torus (non-split torus).

Given a torus  $T \subset Sp$ , the decomposition  $\mathcal{H} = \bigoplus \mathcal{H}_\chi$  into character spaces depends on the type of  $T$ . If  $T$  is a split torus then  $\dim \mathcal{H}_\chi = 1$  unless  $\chi = \sigma$ , where  $\sigma$  is the unique quadratic character of  $T$  (also called *Legendre* character), in the latter case  $\dim \mathcal{H}_\sigma = 2$ . If  $T$  is a non-split torus then  $\dim \mathcal{H}_\chi = 1$  for every character  $\chi$  which appears in the decomposition, in this case the quadratic character  $\sigma$  does not appear in the decomposition [GH2].

1) *Geometric projectors:* Below we state the main technical statement of this paper which roughly says that the character spaces  $\mathcal{H}_\chi$  can be geometrized.

Given a torus  $T \subset Sp$  and a character  $\chi \in T^\vee$ ,  $\chi \neq \sigma$ , we denote by  $P_\chi$  the orthogonal projector on the space  $\mathcal{H}_\chi$ . Let  $W_{P_\chi}$  be the Weyl transform of  $P_\chi$ , we denote by  $W_\chi$  the normalized function  $W_\chi = \#(T) \cdot W_{P_\chi}$ .

*Theorem IV-A.1:* There exists geometrically irreducible [1]-perverse Weil sheaf  $\mathcal{W}_\chi$  of pure weight zero on  $\mathbf{V}$  such that

$$W_\chi = f^{\mathcal{W}_\chi}.$$

For a proof see Appendix A.1.

##### B. The oscillator system

Given a torus  $T \subset Sp$ , choosing for every character  $\chi \in T^\vee$ ,  $\chi \neq \sigma$ , a unit vector  $\varphi_\chi \in \mathcal{H}_\chi$  we obtain a collection of orthonormal vectors  $\mathcal{B}_T = \{\varphi_\chi : \chi \neq \sigma\}$ . We note, that when  $T$  is non-split, the system  $\mathcal{B}_T$  is an orthonormal basis. Considering the union of all these collections, we obtain the oscillator system

$$\mathfrak{S}_O = \{\varphi \in \mathcal{B}_T : T \subset Sp\}.$$

It will be convenient to separate the system  $\mathfrak{S}_O$  into two subsystems  $\mathfrak{S}_O^s$  and  $\mathfrak{S}_O^{ns}$  which correspond to the split tori and the non-split tori respectively. The subsystem  $\mathfrak{S}_O^s$  consists

of  $\frac{q(q+1)}{2}$  collections, each consisting of  $q-2$  orthonormal vectors, altogether  $\#\mathfrak{S}_O^s = \frac{q(q+1)(q-2)}{2}$ . The non-split subsystem  $\mathfrak{S}_O^{ns}$  consists of  $q(q-1)$  collections each consisting of  $q$  orthonormal vectors, altogether  $\#\mathfrak{S}_O^{ns} = q^2(q-1)$ . The properties of  $\mathfrak{S}_O$  are summarized in the following propositions.

*Proposition IV-B.1 (Auto-correlations):* For every  $\varphi \in \mathcal{B}_T$

$$|A_\varphi(h)| = \begin{cases} 1, & h \in Z, \\ \leq \frac{2}{\sqrt{q}}, & h \notin Z. \end{cases}$$

*Proposition IV-B.2 (Cross-correlations):* For every  $\varphi \in \mathcal{B}_T$  and  $\varphi' \in \mathcal{B}_{T'}$

$$|m_{\varphi, \varphi'}(h)| \leq \frac{4}{\sqrt{q}}.$$

*Proposition IV-B.3 (Supermum):* Let  $S = (L, M)$  be a splitting, then for every  $\varphi \in \mathcal{B}_T$

$$\sup_{x \in L} |\varphi(x)| \leq \frac{2}{\sqrt{q}},$$

where  $\varphi$  is realized as a function  $\varphi \in \mathcal{H}_S = \mathbb{C}(L)$ .

*Remark IV-B.4:* In Proposition IV-B.2, if  $T = T'$ ,  $\varphi \neq \varphi'$ , then there exists an improved estimate

$$|m_{\varphi, \varphi'}(h)| \leq \frac{2}{\sqrt{q}}.$$

In the following subsections we will explain the main arguments in the proofs of these propositions. The proofs of the technical statements are given in the appendix.

##### C. Proof of Proposition IV-B.1

Let  $T \subset Sp$  be a torus and  $\chi \in T^\vee$ ,  $\chi \neq \sigma$ . Let  $\varphi = \varphi_\chi \in \mathcal{H}_\chi$  be a unit vector. Clearly  $m_{\varphi, \varphi}(h) = 1$  when  $h \in Z$ . We would like to show that  $|m_{\varphi, \varphi}(h)| \leq \frac{2}{\sqrt{q}}$  when  $h \notin Z$ . In order to do this we will write an explicit expression for  $m_{\varphi, \varphi}(h)$  and then we will use geometric techniques to estimate it.

1) *Explicit expression of the matrix coefficient.* : Recall  $m_{\varphi, \varphi}(h) = \langle \varphi | \pi(h) \varphi \rangle$ . Since  $\dim \mathcal{H}_\chi = 1$  we have  $\langle \varphi | \pi(h) \varphi \rangle = \text{Tr}(P_\chi \pi(h))$ , which, in turn, is equal to  $\dim \mathcal{H} \cdot W_{P_\chi}(h^{-1})$ , where  $P_\chi$  is the orthogonal projector on the subspace  $\mathcal{H}_\chi$ . The projector  $P_\chi$  can be written as  $P_\chi = \frac{1}{\#T} \sum_{a \in T} \bar{\chi}(a) \rho(a)$ , therefore we can write

$$m_{\varphi, \varphi}(h) = \frac{\dim \mathcal{H}}{\#T} \cdot \sum_{a \in T} \bar{\chi}(a) K_a(h) = o(1) \cdot \sum_{a \in T} \bar{\chi}(a) K_a(h),$$

where we recall that  $\dim \mathcal{H} = q$ , and  $\#T = q \pm 1$ , depending on the type of the torus  $T$ .

2) *Estimation:* It is enough to estimate  $m_{\varphi, \varphi}(h)$  when  $h = v \in V$ ,  $v \neq 0$ .

*Proposition IV-C.1:* Let  $v \in V$ ,  $v \neq 0$ , then

$$\left| \sum_{a \in T} \bar{\chi}(a) K_a(v) \right| \leq \frac{2}{\sqrt{q}}.$$

As a result we obtain

$$|m_{\varphi, \varphi}(v)| = \begin{cases} 1, & v = 0, \\ \leq c \cdot \frac{2}{\sqrt{q}}, & v \neq 0, \end{cases}$$

where  $c = \frac{q}{q-1}$  when  $T$  is split and  $c = \frac{q}{q+1}$  when  $T$  is non-split.



#### D. Proof of Proposition IV-B.2

Let  $T_i \subset Sp$ ,  $i = 1, 2$ , be a pair of tori and let  $\chi_i \in T_i^\vee$ ,  $\chi_i \neq \sigma_i$ . We choose unit vectors  $\varphi_i = \varphi_{\chi_i} \in \mathcal{H}_{\chi_i}$   $i = 1, 2$ , and would like to show that

$$|m_{\varphi_1, \varphi_2}(h)| \leq \frac{4}{\sqrt{q}},$$

for every  $h \in H$ .

Let  $P_i = P_{\chi_i}$  denote the orthogonal projector on  $\mathcal{H}_{\chi_i}$ . Our approach will consists of two steps, first we write  $m_{\varphi_1, \varphi_2}(h)$  in terms of  $W_{P_i}$  and, second, we use Theorem IV-A.1 to obtain an estimate. Explicit calculation reveals that

$$|m_{\varphi_1, \varphi_2}(h)|^2 = \dim \mathcal{H} \cdot |W_{P_1} * Ad_h W_{P_2}|(0),$$

for every  $h \in H$ .

Let us denote by  $W_i$  the normalized function  $\#T_i \cdot W_{P_i}$ .

**Proposition IV-D.1:** We have  $|W_1 * Ad_h W_2|(0) \leq 16$ .

Now we can write

$$\begin{aligned} |m_{\varphi_1, \varphi_2}(h)|^2 &= \dim \mathcal{H} \cdot |W_{P_1} * Ad_h W_{P_2}|(0) \\ &\leq \frac{\dim \mathcal{H}}{\#T_1 \cdot \#T_2} |W_1 * Ad_h W_2|(0) \\ &\leq o(1) \frac{16}{q}, \end{aligned}$$

which implies  $|m_{\varphi_1, \varphi_2}(h)| \leq o(1) \frac{4}{\sqrt{q}}$ .

#### E. Proof of proposition IV-D.1

Let us denote by  $C$  the scalar  $W_1 * Ad_h W_2(0)$ . Using Theorem IV-A.1 we can describe the scalar  $C$  geometrically. Let  $\mathcal{W}_i$  be the sheaf on  $\mathbf{V}$  associated to  $W_i$ . We define the object  $\mathcal{C} \in \mathbf{D}(\mathbf{pt})$  by

$$\mathcal{C} = (W_1 * Ad_h W_2)|_0.$$

The object  $\mathcal{C}$  is a Weil object and by the Grothendieck's Lefschetz trace formula [G] we have  $C = f^C$ . Since  $\mathcal{W}_1$  and  $Ad_h \mathcal{W}_2$  are of pure weight zero and the operation of convolution and restriction do not increase weight [D], this implies that  $\mathcal{C}$  is of mixed weight  $w(\mathcal{C}) \leq 0$ . In more concrete terms,  $\mathcal{C}$  is a complex of vector spaces such that

$$|\text{e.v.}(Fr|_{H^i(\mathcal{C})})| \leq \sqrt{q}^i.$$

**Lemma IV-E.1 (Vanishing lemma):** We have

$$\dim H^i(\mathcal{C}) \leq \begin{cases} 0, & i \neq 0, \\ 16, & i = 0. \end{cases}$$

Now we can write  $|C| = |\chi_{Fr}(\mathcal{C})| = |Tr(Fr|_{H^0(\mathcal{C})})| \leq 16$  which concludes the proof of the proposition.

1) *Proof of the vanishing lemma:* The action of  $\mathbf{T}_i$  on  $\mathbf{V}$  yields a decomposition  $\mathbf{S}_i : \mathbf{V} = \mathbf{L}_i \times \mathbf{M}_i$  into eigenspaces. Denote  $\Pi_i = \Pi_{\mathbf{S}_i}$  and  $F = F_{\mathbf{S}_2, \mathbf{S}_1}$ . We have

$$\begin{aligned} \mathcal{C} &\simeq Tr[\Pi_2(\mathcal{W}_1) \circ Ad_h \Pi_2(\mathcal{W}_2)] \\ &\simeq Tr[F(\Pi_1(\mathcal{W}_1)) \circ Ad_h \Pi_2(\mathcal{W}_2)]. \end{aligned}$$

Our next goal is to give an explicit description of  $\Pi_i(\mathcal{W}_i)$  as sheaves on  $\mathbf{L}_i \times \mathbf{L}_i$ . For this, we choose vectors  $l_i \in \mathbf{L}_i$  and identify  $\tau_i : \mathbf{T}_i \xrightarrow{\sim} \mathbf{L}_i$ . Denote  $\mathcal{F}_{\chi_i} = \tau_{i!}(\mathcal{L}_{\bar{\chi}_i \sigma})$ .

**Lemma IV-E.2:** There exists an isomorphism  $\Pi_i(\mathcal{W}_i) \simeq \mathcal{F}_{\chi_i} \boxtimes \mathcal{F}_{\bar{\chi}_i}$ .

Now we can write

$$Tr[F(\Pi_1(\mathcal{W}_1)) \circ Ad_h \Pi_2(\mathcal{W}_2)] \simeq$$

$$\int_{l \in \mathbf{L}_2} \left( F^L(\mathcal{F}_{\chi_1}) \otimes \mathcal{F}_{\bar{\chi}_2}^{h^{-1}} \right) [1] \otimes \int_{l \in \mathbf{L}_2} \left( F^R(\mathcal{F}_{\chi_1}) \otimes \mathcal{F}_{\chi_2}^h \right) [1],$$

where  $\mathcal{F}_{\chi_2}^h$  and  $\mathcal{F}_{\bar{\chi}_2}^{h^{-1}}$  stand for  $h \triangleright \mathcal{F}_{\chi_2}$  and  $h^{-1} \triangleright \mathcal{F}_{\bar{\chi}_2}$  respectively. The result now follows from the following lemma

**Lemma IV-E.3:** We have

$$\begin{aligned} \dim H^i \left( \int_{l \in \mathbf{L}_2} \left( F^L(\mathcal{F}_{\chi_1}) \otimes \mathcal{F}_{\bar{\chi}_2}^{h^{-1}} \right) \right) &\leq \begin{cases} 4, & i = 1, \\ 0, & i = 0, \end{cases} \\ \dim H^i \left( \int_{l \in \mathbf{L}_2} \left( F^R(\mathcal{F}_{\bar{\chi}_1}) \otimes \mathcal{F}_{\chi_2}^h \right) \right) &\leq \begin{cases} 4, & i = 1, \\ 0, & i = 0. \end{cases} \end{aligned}$$

This concludes the proof of the vanishing lemma.

#### F. Proof of Proposition IV-B.3

Let  $T \subset Sp$  be a torus and  $\chi \in T^\vee$ ,  $\chi \neq \sigma$ . We choose a unit vector  $\varphi = \varphi_\chi \in \mathcal{H}_\chi$ . Let  $S = (L, M)$  be a Lagrangian splitting and  $(\pi_S, \bar{H}, \mathcal{H}_S)$  be the associated Schrödinger model of the Heisenberg representation. We consider  $\varphi$  as a function  $\varphi \in \mathcal{H}_S = \mathbb{C}(L)$  and would like to prove the following estimate

$$|\varphi(x)| \leq \frac{2}{\sqrt{q}}$$

for every  $x \in L$ .

Let us assume that both Lagrangians  $L$  and  $M$  are not fixed by  $T$ , the case when either  $L$  or  $M$  are fixed by  $T$  is easier. Our approach will consists of two steps, first we interpret the quantity  $\varepsilon = |\varphi(x)|$  in representation theoretic terms and then we use geometry to obtain an estimate. Recall that we denoted by  $P_\chi$  the orthogonal projector on  $\mathcal{H}_\chi$ , let us denote by  $P_x$  the orthogonal projector on the  $x$ -eigenspace  $\mathcal{H}_x = \mathbb{C}\delta_x \subset \mathcal{H}_S$ . Explicit calculation reveals that

$$\varepsilon^2 = Tr(P_\chi \cdot P_x).$$

It is enough to show that

$$|\varepsilon|^2 \leq \frac{4}{q}.$$

We can write

$$Tr(P_\chi P_x) = W_{P_\chi} * W_{P_x}(0).$$

Consider the normalized functions  $W_\chi = \#T \cdot W_{P_\chi}$  and  $W_x = \#L \cdot W_{P_x}$ . The result follows from the following proposition

**Proposition IV-F.1:** We have  $|W_\chi * W_x(0)| \leq 4q$ .

## APPENDIX

## A. Proofs of technical statements

1) *Proof of Theorem IV-A.1:* Let  $\mathbf{T} \subset \mathbf{Sp}$  be the algebraic torus such that  $T = \mathbf{T}(\mathbb{F}_q)$ . Let  $\mathcal{K}$  be the Weil representation sheaf on  $\mathbf{Sp} \times \mathbf{V}$  (Theorem III-D.1). Let us denote by  $\mathcal{K}_{\mathbf{T}}$  and  $\mathcal{K}_{\mathbf{T}^\times}$  the restrictions of  $\mathcal{K}$  to the subvarieties  $\mathbf{T} \times \mathbf{V}$  and  $\mathbf{T}^\times \times \mathbf{V}$  respectively, where  $\mathbf{T}^\times$  denotes the punctured torus  $\mathbf{T} - \{1\}$ . We define

$$\mathcal{W}_\chi(v) = \int_{a \in \mathbf{T}} \mathcal{L}_{\overline{\chi}}(a) \otimes \mathcal{K}_{\mathbf{T}}(a, v).$$

Equivalently, we can write  $\mathcal{W}_\chi(v) = \pi_!(\mathcal{L}_\chi \otimes \mathcal{K}_{\mathbf{T}})$ , where  $\pi : \mathbf{T} \times \mathbf{V} \rightarrow \mathbf{V}$  is the projector on the  $\mathbf{V}$ -coordinate. By the Grothendieck's Lefschetz trace formula [G] we have  $f^{\mathcal{W}_\chi} = W_\chi$ . We would like to show that  $\mathcal{W}_\chi$  is geometrically irreducible [1]-perverse.

*Lemma A.1:* The sheaf  $\mathcal{K}_{\mathbf{T}}$  is geometrically irreducible  $[\dim \mathbf{T}]$ -perverse.

Since the functor  $\pi_!$  is perverse left exact [BBD] hence, using the previous lemma, we obtain that  $\mathcal{W}_\chi \in \mathcal{D}^{p, \geq 1}$ . It is enough to show that  $\mathcal{W}_\chi \in \mathcal{D}^{p, \leq 1}$ .

Consider the stratification  $\mathbf{V} = \mathbf{U}_0 \cup \mathbf{U}_1 \cup \mathbf{U}_2$ , where  $\mathbf{U}_2$  is the open subvariety consisting of all elements  $v \in \mathbf{V}$  which are not eigenvectors with respect to the action of  $\mathbf{T}$ ,  $\mathbf{U}_1 = \mathbf{V} - \mathbf{U}_2 - \{0\}$  and  $\mathbf{U}_0 = \{0\}$ .

*Lemma A.2:* We have  $H^i(\mathcal{W}_\chi) = 0$  for  $i \neq -1, 0$  and

$$\begin{aligned} \dim \operatorname{Supp}(H^{-1}(\mathcal{W}_\chi)) &= 2, \\ \dim \operatorname{Supp}(H^0(\mathcal{W}_\chi)) &= 0. \end{aligned}$$

The restrictions on the support of the cohomologies of  $\mathcal{W}_\chi$  imply that  $\mathcal{W}_\chi \in \mathcal{D}^{p, \leq 1}$ , in fact, it implies that  $\mathcal{W}_\chi$  is the middle extension of its restriction to any open subvariety of  $\mathbf{V}$ . In particular,  $\mathcal{W}_\chi = j_{!*}(\mathcal{W}_{\chi|_{\mathbf{U}_2}})$  for  $j : \mathbf{U}_2 \hookrightarrow \mathbf{V}$  and because  $\mathcal{W}_{\chi|_{\mathbf{U}_2}}$  is irreducible [1]-perverse sheaf,  $\mathcal{W}_\chi$  is either. This concludes the proof of the theorem.

a) *Proof of Lemma A.1:* The statement follows from the following two properties of  $\mathcal{K}_{\mathbf{T}}$ . First, the restriction  $\mathcal{K}_{\mathbf{T}|_{\mathbf{T}^\times}} = \mathcal{K}_{\mathbf{T}^\times}$  is geometrically irreducible [1]-perverse sheaf, in fact,  $\mathcal{K}_{\mathbf{T}^\times}$  is smooth. Second, there exists an isomorphism  $m^*\mathcal{K}_{\mathbf{T}} \simeq \mathcal{K}_{\mathbf{T}^\times} * \mathcal{K}_{\mathbf{T}^\times}$ . Now, consider the map  $m : \mathbf{T}^\times \times \mathbf{T}^\times \times \mathbf{V} \rightarrow \mathbf{T} \times \mathbf{V}$  which is smooth and surjective. It is enough to show that the pullback  $m^*\mathcal{K}_{\mathbf{T}}$  is irreducible  $[\dim(\mathbf{T}^\times \times \mathbf{T}^\times)]$ -perverse. Using the second property we have  $m^*\mathcal{K}_{\mathbf{T}} \simeq \mathcal{K}_{\mathbf{T}^\times} * \mathcal{K}_{\mathbf{T}^\times}$  where the right hand side is principally an application of Fourier transform which maintains perversity [KL] so the statement follows. This concludes the proof of the Lemma.

b) *Proof of Lemma A.2:* We will show that  $\operatorname{Supp}(H^{-1}(\mathcal{W}_\chi)) \subset \mathbf{U}_2 \cup \mathbf{U}_1$  and that  $\operatorname{Supp}(H^0(\mathcal{W}_\chi)) \subset \mathbf{U}_0$ . First, let  $v \in \mathbf{U}_2$ , we have

$$\mathcal{W}_\chi(v) = \int_{a \in \mathbf{T}^\times} \mathcal{L}_{\overline{\chi}}(a) \otimes \mathcal{L}_\mu(a) \otimes \mathcal{L}_\psi\left(\frac{1}{4}\omega(\kappa(a)v, v)\right) [2](1).$$

Standard cohomological techniques yields that  $\mathcal{W}_\chi(v)$  is concentrated at degree  $-1$ . In fact,  $\mathcal{W}_{\chi|_{\mathbf{U}_2}}$  is an irreducible [1]-perverse sheaf since it is principally a Fourier transform of the irreducible perverse sheaf  $\mathcal{L}_{\overline{\chi}} \otimes \mathcal{L}_\mu$ . Second, let  $v \in \mathbf{U}_1$ , we

have  $\mathcal{W}_\chi(v) = \int_{\mathbf{T}^\times} \mathcal{L}_{\overline{\chi}} \otimes \mathcal{L}_\mu [2](1)$ . Denote  $j : \mathbf{T}^\times \hookrightarrow \mathbf{T}$  and consider the exact triangle of sheaves on  $\mathbf{T}$

$$(\mathcal{L}_{\overline{\chi}} \otimes \mathcal{L}_\mu)_{|1}[-1] \rightarrow j_! \left\{ (\mathcal{L}_{\overline{\chi}} \otimes \mathcal{L}_\mu)_{|\mathbf{T}^\times} \right\} \rightarrow \mathcal{L}_{\overline{\chi}} \otimes \mathcal{L}_\mu.$$

Applying  $\pi_! [2](1)$  to all the terms in the previous exact sequence we obtain that  $\mathcal{W}_\chi(v) = (\mathcal{L}_\chi \otimes \mathcal{L}_\mu)_{|1} [1](1)$ , implying in particular that it is concentrated at degree  $-1$ . Finally, let  $v \in \mathbf{U}_0$ , we have  $\mathcal{W}_\chi(0) = \int_{a \in \mathbf{T}} \mathcal{L}_{\overline{\chi}}(a) \otimes \mathcal{K}_{\mathbf{T}}(a, 0)$ . Using the exact triangle

$$j_! \left\{ (\mathcal{L}_{\overline{\chi}} \otimes \mathcal{K}_{\mathbf{T}})_{|\mathbf{T}^\times \times 0} \right\} \rightarrow (\mathcal{L}_{\overline{\chi}} \otimes \mathcal{K}_{\mathbf{T}})_{|\mathbf{T} \times 0} \rightarrow \delta_1,$$

we obtain  $\pi_! \left\{ (\mathcal{L}_{\overline{\chi}} \otimes \mathcal{K}_{\mathbf{T}})_{|\mathbf{T}^\times \times 0} \right\}$  is concentrated at degree  $-1, 0$ .

2) *Proof of proposition IV-C.1:* Denote  $a_\chi = \sum_{a \in T} \overline{\chi}(a) K(a, v)$ . Using formula (II-E.3) we can write

$$\sum_{a \in T} \overline{\chi}(a) K(a, v) = \frac{1}{\dim \mathcal{H}} \sum_{a \in T^\times} \overline{\chi}(a) \mu(a) \psi\left(\frac{1}{4}\omega(\kappa(a)v, v)\right),$$

where  $T^\times$  denotes the punctured torus  $T^\times = T - \{1\}$ . The last expression can be estimated using standard cohomological techniques. We have  $a_\chi = f^{\mathcal{A}_\chi}$  where

$$\mathcal{A}_\chi = \int_{a \in \mathbf{T}^\times} \mathcal{L}_{\overline{\chi}}(a) \otimes \mathcal{L}_\mu(a) \otimes \mathcal{L}_\psi\left(\frac{1}{4}\omega(\kappa(a)v, v)\right) (1).$$

Since integration with compact support does not increase weight [D]  $\mathcal{A}_\chi$  is a Weil object in  $\mathcal{D}(\mathbf{pt})$  of mixed weight  $w(\mathcal{A}_\chi) \leq 0$ . Concretely, this means that  $\mathcal{A}_\chi$  is merely a complex of vector spaces such that  $|\text{e.v.}(Fr_{|H^i(\mathcal{A}_\chi)})| \leq \sqrt{q}^i$ .

*Lemma A.3:* We have

$$\dim H^i(\mathcal{A}_\chi) = \begin{cases} 2, & i = 1, \\ 0, & i \neq 1. \end{cases}$$

Now we can write  $|a_\chi| = |Tr(Fr_{|H^i(\mathcal{A}_\chi)})| \leq \dim H^i(\mathcal{A}_\chi) \cdot \frac{\sqrt{q}}{q} = \frac{2}{\sqrt{q}}$ . This concludes the proof of the proposition.

a) *Proof of Lemma A.3:* Denote  $\mathcal{K}_\chi = \mathcal{L}_{\overline{\chi}}(a) \otimes \mathcal{L}_\mu(a) \otimes \mathcal{L}_\psi\left(\frac{1}{4}\omega(\kappa(a)v, v)\right)$ . Identifying  $\mathbf{V} \simeq \mathbb{A}_m^2$  and  $\mathbf{T}^\times \simeq \mathbb{G}_m^\times - \{1\}$  we let  $v = (x, y) \neq (0, 0)$ . It is not hard to verify that the sheaf  $\mathcal{L}_\mu$ , considered as a plain topological sheaf, is isomorphic to the Kummer sheaf  $\mathcal{L}_\sigma$  on  $\mathbb{G}_m^\times$  and the sheaf  $\mathcal{L}_\psi\left(\frac{1}{4}\omega(\kappa(a)v, v)\right)$  is isomorphic to  $\mathcal{L}_\psi\left(\frac{1}{2}xy \frac{a+1}{a-1}\right)$ . We can deduce that  $\mathcal{K}_\chi$  is tame both at 0 and  $\infty$  and it is wild at 1 with a single break 1. Since  $\mathcal{K}_\chi$  is irreducible and non-constant, the integral  $\mathcal{A}_\chi = \int_{a \in \mathbf{T}^\times} \mathcal{K}_\chi$  is concentrated at degree 1, in addition

$$\begin{aligned} \dim H^1(\mathcal{A}_\chi) &= \text{Swan}_1 \mathcal{K}_\chi - \chi(\mathbb{G}_m^\times) \\ &= 1 + 1 = 2. \end{aligned}$$

This concludes the proof of the lemma.

3) *Proof of Lemma IV-E.2:* Fix  $i$ , denote  $\mathbf{T} = \mathbf{T}_i$ ,  $\chi = \chi_i$ ,  $\Pi = \Pi_i$  and  $\mathbf{L} = \mathbf{L}_i$ ,  $\mathbf{M} = \mathbf{M}_i$ . Since  $\mathcal{W}_\chi$  is irreducible [1]-perverse on  $\mathbf{L} \times \mathbf{M}$  hence  $\Pi(\mathcal{W}_\chi)$  is irreducible [2]-perverse on  $\mathbf{L} \times \mathbf{L}$ , therefore it is enough to show  $\Pi(\mathcal{W}_\chi)(x, y) \simeq \mathcal{F}_{\overline{\chi}}(x) \boxtimes \mathcal{F}_\chi(y)$  on any open subvariety of  $\mathbf{L} \times \mathbf{L}$ . Let  $\mathbf{U} \subset \mathbf{L} \times \mathbf{L}$  denote the open subvariety consisting of  $(x, y) \in \mathbf{L} \times \mathbf{L}$  so that  $x, y \neq 0$  and  $x \neq y$ . We have

$$\Pi(\mathcal{W}_\chi)(x, y) = \int_{m \in \mathbf{M}} \mathcal{L}_\psi \left( \frac{1}{2} \omega(x + y, m) \right) \otimes \mathcal{W}_\chi(y - x, m)$$

If we let  $\tau : \mathbf{T} \rightarrow GL(\mathbf{L})$  denote the action of  $\mathbf{T}$  on  $\mathbf{L}$  then explicit computation reveals that

$$\begin{aligned} \Pi(\mathcal{W}_\chi)(x, y) &\simeq \int_{m \in \mathbf{M}} \int_{a \in \mathbf{T}^\times} \mathcal{L}_{\overline{\chi}\sigma}(a) \otimes \mathcal{L}_\psi \left( \omega \left( \frac{\tau(a)y - x}{\tau(a) - 1}, m \right) \right) [2] \\ &\simeq \int_{a \in \mathbf{T}^\times} \mathcal{L}_{\overline{\chi}\sigma}(a) \otimes \delta_{\{\tau(a) = \frac{x}{y}\}} [-2][2] \\ &\simeq \int_{a \in \mathbf{T}^\times} \mathcal{L}_{\overline{\chi}\sigma}(a) \otimes \delta_{\{\tau(a) = \frac{x}{y}\}}, \end{aligned}$$

and the last term in is isomorphic to  $\mathcal{F}_{\overline{\chi}}(x) \boxtimes \mathcal{F}_\chi(y)$ . This concludes the proof of the lemma.

4) *Proof of Lemma IV-E.3:* We will prove the second estimate, the first one is proved in exactly the same manner. Let  $h = (v, 0)$  and write  $v = (l_2, m_2)$ . First we study  $\mathcal{F}_{\chi_2}^h$ . We have

$$\mathcal{F}_{\chi_2}^h(x) = \mathcal{L}_\psi \left( \frac{1}{2} \omega(l_2, m_2) + \omega(x, m_2) \right) \otimes \mathcal{F}_{\chi_2}(x + l_2).$$

The sheaf  $\mathcal{F}_{\chi_2}^h$  is irreducible [1]-perverse, smooth of rank 1 on the open subvariety  $\mathbf{L}_2 - \{l_2\}$ . In addition, it is tame at  $l_2$  and wildly ramified at  $\infty$  with a single break equal 1.

Second, we study  $F^R(\mathcal{F}_{\overline{\chi}_1})$ . We assume that we are in the case when  $A : \mathbf{L}_1 \times \mathbf{M}_1 \rightarrow \mathbf{L}_2 \times \mathbf{M}_2$  satisfies  $A_{21} \neq 0$ , the other case is easier and therefore is omitted. We have

$$F^R(\mathcal{F}_{\overline{\chi}_1})(x) = \int_{y \in \mathbf{L}_1} \mathcal{L}_\psi \left( \frac{1}{2} \omega(Cy - Bx, y) - \frac{1}{2} \omega(Dx, x) \right) \otimes \mathcal{F}_{\overline{\chi}_1}(y) [1].$$

We assume  $C \neq 0$ , the analysis when  $C = 0$  is easier therefore is omitted. Denote  $\mathcal{G}_1 = \mathcal{L}_\psi \left( \frac{1}{2} \omega(Cy, y) \right) \otimes \mathcal{F}_{\overline{\chi}_1}$ . The sheaf  $\mathcal{G}_1$  is smooth of rank 1 on  $\mathbf{L}_1 - \{0\}$ , it is tame at 0, wild at  $\infty$  with a single break equal 2. Denote  $\mathcal{G}_2 = \int_{y \in \mathbf{L}_1} \mathcal{L}_\psi \left( -\frac{1}{2} \omega(Bx, y) \right) \otimes \mathcal{G}_1(y) [1]$ . The sheaf  $\mathcal{G}_2$  is irreducible [1]-perverse since it is the (normalized) Fourier transform of  $\mathcal{G}_1$ . Moreover, for every  $x \in \mathbf{L}_2$ ,  $\mathcal{G}_2(x)$  is concentrated at degree 0 and  $\dim \mathcal{G}_2(x) = \text{Swan}_\infty(\mathcal{G}_1) = 2$ , hence  $\mathcal{G}_2$  is smooth of rank 2.

*Lemma A.4:* We have  $\mathcal{G}_2(\infty) = \mathcal{G}_2(\infty)_{\text{tame}} \oplus \mathcal{G}_2(\infty)_{\text{break}=2}$ , both components are of dimension 1.

Denote  $\mathcal{G}_3 = \mathcal{L}_\psi \left( -\frac{1}{2} \omega(Dx, x) \right) \otimes \mathcal{G}_2$ . The sheaf  $\mathcal{G}_3$  is irreducible [1]-perverse, smooth of rank 2 with break decomposition  $\mathcal{G}_3(\infty) = (\mathcal{G}_3(\infty))_2 \oplus (\mathcal{G}_3(\infty))_{\leq 2}$ , both components are of dimension 1. Finally, denote  $\mathcal{G}_4 = \mathcal{G}_3 \otimes \mathcal{F}_{\chi_2}^h$ . The sheaf  $\mathcal{G}_4$  is irreducible [1]-perverse, smooth of rank 2 on the open subvariety  $\mathbf{L}_2 - \{l_2\}$ , it is tame at  $l_2$  with break decomposition

$\mathcal{G}_4(\infty) = \mathcal{G}_4(\infty)_2 \oplus \mathcal{G}_4(\infty)_{\leq 2}$ , both components are of dimension 1. Now, considering the integral  $\int_{x \in \mathbf{L}_2} \mathcal{G}_4$ , it is concentrated at degree 1 and

$$\dim H^1 \left( \int_{x \in \mathbf{L}_2} \mathcal{G}_4 \right) = \text{Swan}_\infty \mathcal{G}_4 - \chi(\mathbb{G}_m) \leq 4.$$

This concludes the proof of the lemma.

a) *Proof of Lemma A.4:* Using the Laumon stationary phase method, the restriction  $\mathcal{G}_2(\infty)$  is a sum of local contributions

$$\mathcal{G}_2(\infty) = FT_\psi \text{loc}(0, \infty)(\mathcal{G}_1(0)) \oplus FT_\psi \text{loc}(\infty, \infty)(\mathcal{G}_1(\infty)).$$

Here  $FT_\psi \text{loc}(t, \infty)$ ,  $t \in \mathbb{P}^1$  denote the Laumon local Fourier functors. The functors  $FT_\psi \text{loc}(t, \infty)$ ,  $t = 0, \infty$  satisfy, in particular, the following properties:

- 1)  $FT_\psi \text{loc}(0, \infty)$  sends a tame sheaf of determinant  $\mathcal{L}_\chi$  to a tame sheaf of determinant  $\mathcal{L}_{\overline{\chi}}$  of the same rank.
- 2)  $FT_\psi \text{loc}(\infty, \infty)$  sends a wild sheaf with a single break  $\frac{a+b}{b}$  of multiplicity  $b$  to a wild sheaf with a single break  $\frac{a+b}{a}$  of multiplicity  $a$ .

Using these two properties we obtain  $\mathcal{G}_2(\infty) = (\mathcal{G}_2(\infty))_{\text{tame}} \oplus (\mathcal{G}_2(\infty))_{\text{break}=2}$  and  $\dim \mathcal{G}_2(\infty)_{\text{tame}} = \dim \mathcal{G}_2(\infty)_{\text{break}=2} = 1$ .

5) *Proof of proposition IV-F.1:* Let us denote by  $C$  the scalar  $W_\chi * W_x(0)$ . We are going to describe an object  $C \in D(\mathbf{pt})$  such that  $C = f^C$ .

*Lemma A.5:* There exist geometrically irreducible [1]-perverse Weil sheaf  $\mathcal{W}_x$  of pure weight 0 on  $\mathbf{V}$  satisfying

$$f^{\mathcal{W}_x} = W_x.$$

Denote  $\mathcal{C} = (\mathcal{W}_\chi * \mathcal{W}_x)_{|0}$ . Since convolution does not increase weight [D],  $\mathcal{C}$  is a Weil object in  $D(\mathbf{pt})$  of mixed weight  $w(\mathcal{C}) \leq 0$ . The result now follows from the following statement:

*Lemma A.6:* We have

$$\dim H^i(\mathcal{C}) = \begin{cases} 4, & i = 2, \\ 0, & i \neq 2. \end{cases}$$

The proof of the proposition now follows easily  $C = f^C = \text{Tr}(Fr_{|H^2(\mathcal{C})}) \leq 4q$ .

a) *Proof of Lemma A.5:* Consider the closed imbedding  $i : \mathbf{M} \rightarrow \mathbf{V}$  and define  $\mathcal{W}_x = i^* \mathcal{L}_{\psi(\omega(\cdot, x))} [2] (1)$ . Clearly,  $\mathcal{W}_x$  is irreducible [1]-perverse of pure weight 0. A direct verification shows that the function  $W_x = f^{\mathcal{W}_x}$  satisfies  $\Pi(W_x) = P_x$ . Concluding the proof of the lemma.

b) *Proof of Lemma A.6:* Let  $\mathbf{V} = \mathbf{A} \times \mathbf{B}$  be the splitting into eigenspaces of  $\mathbf{T}$ . Denote  $\Pi = \Pi_{\mathbf{S}}$ . We have

$$\mathcal{C} \simeq \text{Tr} \{ \Pi(\mathcal{W}_\chi) \circ \Pi(\mathcal{W}_x) \}.$$

Both  $\Pi(\mathcal{W}_\chi)$  and  $\Pi(\mathcal{W}_x)$  are irreducible [2]-perverse and can be calculated explicitly. We know  $\Pi(\mathcal{W}_\chi) \simeq \mathcal{F}_\chi \boxtimes \mathcal{F}_{\overline{\chi}}$  (Lemma IV-E.2). We have

$$\Pi(\mathcal{W}_x)(a_1, a_2) \simeq \int_{b \in \mathbf{B}} \mathcal{L}_\psi \left( \frac{1}{2} \omega(a_1 + a_2, b) \right) \otimes \mathcal{W}_x(a_2 - a_1, b).$$

Let  $R : \mathbf{A} \rightarrow \mathbf{B}$  be the linear map characterized by the property that  $\omega(a, x) = \omega(R(a), x)$  for every  $a \in \mathbf{A}$ . We obtain

$$\begin{aligned} \Pi(\mathcal{W}_x)(a_1, a_2) &\simeq \mathcal{L}_\psi \left( \frac{1}{2} \omega(R(a_2 - a_1), a_1 + a_2) \right) \\ &\quad \otimes \mathcal{L}_\psi \left( \omega((I - R)(a_2 - a_1), x) \right) \\ &\simeq \mathcal{F}_x(a_1) \boxtimes \overline{\mathcal{F}_x}(a_2), \end{aligned}$$

where

$$\begin{aligned} \mathcal{F}_x(a_2) &\simeq \mathcal{L}_\psi \left( \frac{1}{2} \omega(R(a_2), a_2) + \omega((I - R)(a_2), x) \right), \\ \overline{\mathcal{F}_x}(a_1) &\simeq \mathcal{L}_\psi \left( -\frac{1}{2} \omega(R(a_1), a_1) - \omega((I - R)(a_1), x) \right). \end{aligned}$$

Therefore we can write

$$\begin{aligned} \mathcal{C} &\simeq \text{Tr} \{ (\mathcal{F}_\chi \boxtimes \overline{\mathcal{F}_\chi}) \circ (\mathcal{F}_x \boxtimes \overline{\mathcal{F}_x}) \} \\ &\simeq \left( \int_{\mathbf{L}} \mathcal{F}_\chi \otimes \overline{\mathcal{F}_x} \right) \otimes \left( \int_{\mathbf{L}} \overline{\mathcal{F}_\chi} \otimes \mathcal{F}_x \right). \end{aligned}$$

The statement now follows from

*Lemma A.7:* We have

$$\begin{aligned} \dim H^i \left( \int_{\mathbf{L}} \mathcal{F}_\chi \otimes \overline{\mathcal{F}_x} \right) &= \begin{cases} 2, & i = 1, \\ 0, & i \neq 1, \end{cases} \\ \dim H^i \left( \int_{\mathbf{L}} \overline{\mathcal{F}_\chi} \otimes \mathcal{F}_x \right) &= \begin{cases} 2, & i = 1, \\ 0, & i \neq 1. \end{cases} \end{aligned}$$

*c) Proof of Lemma A.7:* The sheaf  $\mathcal{F}_\chi$  is irreducible perverse, smooth of rank 1 on  $\mathbf{L} - \{0\}$ , tame at 0 and  $\infty$ . The sheaf  $\overline{\mathcal{F}_x}$  is irreducible perverse, smooth of rank 1, wild at  $\infty$  with a single break equal 2. Therefore, the sheaf  $\mathcal{G} = \mathcal{F}_\chi \otimes \overline{\mathcal{F}_x}$  is irreducible perverse, smooth of rank 1 on  $\mathbf{L} - \{0\}$ , tame at 0, wild at  $\infty$  with a single break equal 2. The integral  $\int_{\mathbf{L}} \mathcal{G}$  is concentrated at cohomological degree 1 and  $\dim H^1 \left( \int_{\mathbf{L}} \mathcal{G} \right) = \text{Swan}_\infty \mathcal{G} - \chi(\mathbb{G}_m) = 2$ . The second estimate is proved in the same manner. This concludes the proof of the lemma.

## B. Construction of the oscillator system

*1) Algorithm:* We describe an explicit algorithm that generates the oscillator system  $\mathfrak{S}_O^s$  associated with the collection of split tori in  $Sp$ .

*a) Tori:* Consider the standard diagonal torus

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}; a \in \mathbb{F}_p^\times \right\}.$$

Every split torus in  $Sp$  is conjugated to the torus  $A$ , which means that the collection  $\mathcal{T}$  of all split tori in  $Sp$  can be written as

$$\mathcal{T} = \{gAg^{-1}; g \in Sp\}.$$

*b) Parametrization:* A direct calculation reveals that every torus in  $\mathcal{T}$  can be written as  $gAg^{-1}$  for an element  $g$  of the form

$$g = \begin{pmatrix} 1 & b \\ c & 1 + bc \end{pmatrix}, \quad b, c \in \mathbb{F}_p. \quad (\text{B.1})$$

If  $b = 0$ , this presentation is unique: In the case  $b \neq 0$ , an element  $\tilde{g}$  represents the same torus as  $g$  if and only if it is of the form

$$\tilde{g} = \begin{pmatrix} 1 & b \\ c & 1 + bc \end{pmatrix} \begin{pmatrix} 0 & -b \\ b^{-1} & 0 \end{pmatrix}.$$

Let us choose a set of elements of the form (B.1) representing each torus in  $\mathcal{T}$  exactly once and denote this set of representative elements by  $R$ .

*c) Generators:* The group  $A$  is a cyclic group and we can find a generator  $g_A$  for  $A$ . This task is simple from the computational perspective, since the group  $A$  is finite, consisting of  $p - 1$  elements.

Now, we make the following two observations. First observation is that the oscillator basis  $\mathcal{B}_A$  is the basis of eigenfunctions of the operator  $\rho(g_A)$ .

The second observation is that, other bases in the oscillator system  $\mathfrak{S}_O^s$  can be obtained from  $\mathcal{B}_A$  by applying elements from the set  $R$ . More specifically, for a torus  $T$  of the form  $T = gAg^{-1}$ ,  $g \in R$ , we have

$$\mathcal{B}_{gAg^{-1}} = \{\rho(g)\varphi; \varphi \in \mathcal{B}_A\}.$$

Concluding, we described the (split) oscillator system

$$\mathfrak{S}_O^s = \{\rho(g)\varphi : g \in R, \varphi \in \mathcal{B}_A\}.$$

*d) Formulas:* We are left to explain how to write explicit formulas (matrices) for the operators  $\rho(g)$ ,  $g \in R$ .

First, we recall that the group  $Sp$  admits a Bruhat decomposition  $Sp = B \cup BwB$ , where  $B$  is the Borel subgroup consisting of upper triangular matrices in  $Sp$  and  $w$  denotes the Weyl element

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Furthermore, the Borel subgroup  $B$  can be written as a product  $B = AU = UA$ , where  $A$  is the standard diagonal torus and  $U$  is the standard unipotent group

$$U = \left\{ \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} : u \in \mathbb{F}_p \right\}.$$

Therefore, we can write the Bruhat decomposition also as  $Sp = UA \cup UA w U$ .

Second, we give an explicit description (which can be easily verified using identity (II-E.1)) of operators in the Weil representation which are associated with different types of elements in  $Sp$ . The operators are specified up to a unitary scalar, which is enough for our needs.

- The standard torus  $A$  acts by (normalized) scaling: An element

$$a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

acts by

$$S_a[f](t) = \sigma(a)f(a^{-1}t),$$

where  $\sigma : \mathbb{F}_p^\times \rightarrow \{\pm 1\}$  is the Legendre character,  $\sigma(a) = a^{\frac{p-1}{2}} \pmod{p}$ .

- The subgroup of strictly lower diagonal elements  $U \subset Sp$  acts by quadratic exponents (chirps): An element

$$u = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix},$$

acts by

$$M_u[f](t) = \psi(-\frac{u}{2}t^2)f(t).$$

where  $\psi : \mathbb{F}_p \rightarrow \mathbb{C}^\times$  is the character  $\psi(t) = e^{\frac{2\pi i}{p}t}$ .

- The Weyl element

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

acts by discrete Fourier transform

$$F[f](w) = \frac{1}{\sqrt{p}} \sum_{t \in \mathbb{F}_p} \psi(wt) f(t).$$

Using the Bruhat decomposition we conclude that every operator  $\rho(g)$ ,  $g \in Sp$ , can be written either in the form  $\rho(g) = M_u \circ S_a$  or in the form  $\rho(g) = M_{u_2} \circ S_a \circ F \circ M_{u_1}$ , where  $M_u, S_a$  and  $F$  are the explicit operators above.

*Example B.1:* For  $g \in R$ , with  $b \neq 0$ , the Bruhat decomposition of  $g$  is given explicitly by

$$g = \begin{pmatrix} 1 & 0 \\ \frac{1+bc}{b} & 1 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b^{-1} & 1 \end{pmatrix},$$

and consequently

$$\rho(g) = M_{\frac{1+bc}{b}} \circ S_b \circ F \circ M_{b^{-1}}.$$

For  $g \in R$ , with  $c = 0$ , we have

$$g = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix},$$

and

$$\rho(g) = M_u.$$

### C. Pseudocode

Below, is given a pseudo-code description of the construction of the (split) oscillator system  $\mathfrak{S}_O^s$ .

- 1) Choose a prime  $p$ .
- 2) Compute generator  $g_A$  for the standard torus  $A$ .
- 3) Diagonalize  $\rho(g_A)$  and obtain the basis of eigenfunctions  $B_A$ .
- 4) For every  $g \in R$ :
- 5) Compute the operator  $\rho(g)$  as follows:
  - a) Calculate the Bruhat decomposition of  $g$ , namely, write  $g$  in the form  $g = u_2 \cdot a \cdot w \cdot u_1$  or  $g = u \cdot a$ .
  - b) Calculate the operator  $\rho(g)$ , namely, take  $\rho(g) = M_{u_2} \circ S_a \circ F \circ M_{u_1}$  or  $\rho(g) = M_u \circ S_a$ .
- 6) Compute the vectors  $\rho(g)\varphi$ , for every  $\varphi \in B_A$  and obtain the system  $B_{gAg^{-1}}$ .

*Remark C.1 (Running time):* It is easy to verify that the time complexity of the algorithm presented above is  $O(p^4 \log p)$ . This is, in fact, an optimal time complexity, since

already to specify  $p^3$  vectors, each of length  $p$ , requires  $p^4$  operations.

**Acknowledgement.** It is a pleasure to thank J. Bernstein for his interest and guidance in the mathematical aspects of this work. We are grateful to S. Golomb and G. Gong for their interest in this project. We thank B. Sturmfels for encouraging us to proceed in this line of research. The first author would like to thank V. Anantharam, A. Grünbaum and A. Sahai for interesting discussions. Finally, the second author is indebted to B. Porat for so many discussions where each tried to understand the cryptic terminology of the other.

### REFERENCES

- [BBD] Beilinson A., Bernstein J. and Deligne P., Faisceaux pervers. *Analysis and topology on singular spaces, I, Asterisque, 100, Soc. Math. France, Paris* (1982), 5–171.
- [C] Chang R.W., Synthesis of Band-Limited Orthogonal Signals for Multichannel Data Transmission. *Bell System Technical Journal* 45 (1966).
- [D] Deligne P., La conjecture de Weil II. *Publ. Math. I.H.E.S* 52 (1981), 313–428.
- [G] Grothendieck A., Formule de Lefschetz et rationalité des fonctions *L. Seminaire Bourbaki, Vol. 9, Exp. No. 279* (1964).
- [Ga] Gaitsgory D., Informal introduction to geometric Langlands. *An introduction to the Langlands program, Jerusalem 2001*, Birkhauser, Boston, MA (2003) 269–281.
- [GG] Golomb, S.W. and Gong G., Signal design for good correlation. For wireless communication, cryptography, and radar. *Cambridge University Press, Cambridge* (2005).
- [GH1] Gurevich S. and Hadani R., The Geometric Weil representation. *Accepted for publication in Selecta Mathematica* (2006).
- [GH2] Gurevich S. and Hadani R., Self-reducibility of the Weil representation and some applications. arXiv:math/0612765 (2005).
- [H1] Howe R., Invariant theory and duality for classical groups over finite fields with applications to their singular representation theory, preprint, Yale University.
- [H2] Howe R., Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries. *Indag. Math. (N.S.)* 16 (2005), no. 3–4, 553–583.
- [HCM] Howard, S. D.; Calderbank, A. R.; Moran W., The finite Heisenberg-Weyl groups in radar and communications. *EURASIP J. Appl. Signal Process.* (2006).
- [K] Katz N. M., Gauss sums, Kloosterman sums, and monodromy groups. *Annals of Mathematics Studies, 116. Princeton University Press, Princeton, N.J.* (1988).
- [KL] Katz N. M. and Laumon G., Transformation de Fourier et majoration de sommes exponentielles. *Inst. Hautes Etudes Sci. Publ. Math. No.* 62 (1985), 361–418.
- [PT] Paterson, K.G. and Tarokh V., On the existence and construction of good codes with low peak-to-average power ratios. *IEEE Trans. Inform. Theory* 46 (2000).
- [V] Viterbi A.J., CDMA: Principles of Spread Spectrum Communication. *Addison-Wesley Wireless Communications* (1995).
- [W] Weil A., Sur certains groupes d'opérateurs unitaires. *Acta Math.* 111 (1964) 143–211.
- [We1] Weyl H., The Classical Groups. Their Invariants and Representations. *Princeton University Press, Princeton, N.J.* (1939).
- [We2] Weyl H., Gruppentheorie und Quantenmechanik. *1st edition Hirzel, Leipzig* (1928).
- [Wo] Woodward P.M., Probability and Information theory, with Applications to Radar. *Pergamon Press, New York* (1953).